

23 October 2003

Military Police

Army in Europe Physical Security Program

***This regulation supersedes USAREUR Regulation 190-13, 25 August 1995, and rescinds
AE Form 190-13D, AE Form 190-13E, AE Form 190-13F,
AE Form 190-13G, AE Form 190-13J-R, and AE Form 190-13K-R.**

For the CG, USAREUR/7A:

MICHAEL L. DODSON
Lieutenant General, USA
*Deputy Commanding General/
Chief of Staff*

Official:



GARY C. MILLER
*Regional Chief Information
Officer - Europe*

Summary. This regulation—

- Establishes the Army in Europe Physical Security Program. This program is part of the Army in Europe Force Protection Program.
- Provides supplemental guidance to DA physical-security publications.
- Must be used with AR 190-5, AR 190-11, AR 190-13, AR 190-16, AR 190-51, DA Pamphlet 190-51, AE Regulation 190-16, and USAREUR Regulation 525-13.
- Was previously published as USAREUR Regulation 190-13.

Applicability. This regulation applies to USAREUR major subordinate and tenant commands (AE Reg 10-5, app A) (including U.S. Army tenant units in USEUCOM that are subject to local requirements) and the United States Army Installation Management Agency, Europe Region Office.

Forms. This regulation prescribes AE Form 190-16A, AE Form 190-13H(G), AE Form 190-13H(I), AE Form 190-13I, and AE Form 190-13L. AE and higher-level forms are available through the Army in Europe Publishing System (AEPUBS).

Supplementation. Commanders will not supplement this regulation without Office of the Provost Marshal (OPM), HQ USAREUR/7A (AEAPM-SO), approval.

Records Management. Records created as a result of processes prescribed by this regulation must be identified, maintained, and disposed of according to AR 25-400-2. Record titles and descriptions are available on the Army Records Information Management System website at <https://www.arims.army.mil>.

Suggested Improvements. The proponent of this regulation is the OPM (AEAPM-SO, DSN 381-7338). Users may suggest improvements to this regulation by sending DA Form 2028 to the OPM, HQ USAREUR/7A (AEAPM-SO), Unit 29931, Bin 153, APO AE 09086-9931.

Distribution. A (AEPUBS).

CONTENTS

CHAPTER 1 INTRODUCTION

- 1-1. Purpose
- 1-2. References
- 1-3. Explanation of Abbreviations
- 1-4. Responsibilities

CHAPTER 2 ARMY IN EUROPE PHYSICAL SECURITY PROGRAM

- 2-1. General
- 2-2. Threat Assessment
- 2-3. Liaison
- 2-4. Physical Security Planning
- 2-5. Physical Security Plan
- 2-6. Standing Operating Procedures
- 2-7. Mission-Essential Vulnerable Areas
- 2-8. Risk Analysis
- 2-9. Restricted Areas
- 2-10. Physical Security Surveys
- 2-11. Physical Security Inspections
- 2-12. Reports of Corrective Action
- 2-13. Report Classification
- 2-14. Waivers and Exceptions
- 2-15. Security Engineering Surveys
- 2-16. New Construction and Major Renovations
- 2-17. Physical Security Personnel
- 2-18. Physical Security Training
- 2-19. Physical Security Credentials

CHAPTER 3 SECURITY OF ARMS, AMMUNITION, AND EXPLOSIVES (AA&E)

- 3-1. Purpose
- 3-2. General
- 3-3. Categories of AA&E
- 3-4. Non-sensitive AA&E
- 3-5. Storage Facilities
- 3-6. Determination of Reliability
- 3-7. Access Control
- 3-8. Key-and-Lock Controls
- 3-9. Consolidated Arms Rooms
- 3-10. Armed-Guard Requirements
- 3-11. Intrusion Detection Systems
- 3-12. Protection of Arms

- 3-13. Storage and Supplemental Controls
- 3-14. Arms Racks and Storage Containers
- 3-15. Security Lighting
- 3-16. Doors, Locks, and Locking Devices
- 3-17. Control of Weapons
- 3-18. Protection of Missiles, Rockets, Ammunition, and Explosives at Unit Level
- 3-19. Weapons and Ammunition Inventories
- 3-20. Reporting Missing or Recovered AA&E
- 3-21. Security of AA&E During Training and On Ships
- 3-22. Commercial Weapons and Ammunition
- 3-23. Privately Owned Weapons and Ammunition
- 3-24. Security Patrols and Checks
- 3-25. Training
- 3-26. In-Transit Security of AA&E

CHAPTER 4

ACCESS CONTROL

- 4-1. Purpose
- 4-2. Access Methods
- 4-3. Access-Control Points
- 4-4. ACP Procedures
- 4-5. Access Controls for Deliveries and Contractor Buses
- 4-6. ACP Guidance
- 4-7. ACP Design Standards
- 4-8. ACP Manning Recommendations

CHAPTER 5

SECURITY OF ARMY PROPERTY AT UNIT AND INSTALLATION LEVEL

- 5-1. General
- 5-2. Communications Security (COMSEC) Material and Controlled Cryptographic Items
- 5-3. Security of Night-Vision Devices
- 5-4. Security of Global Positioning System and Precision Lightweight Receivers
- 5-5. Security of U.S. Army-Issued Bayonets
- 5-6. Storage Structure Security
- 5-7. Keys, Locks, Locking Devices (Including Hasps and Chains), and Protective Seals
- 5-8. Key Custodian and Alternate Custodian
- 5-9. Key Control Register
- 5-10. Key Depository
- 5-11. Locks
- 5-12. Key-and-Lock Accountability
- 5-13. Additional Key-and-Lock Controls for IDS and Key Containers
- 5-14. Chains
- 5-15. Use and Control of Protective Seals

CHAPTER 6

PHYSICAL SECURITY EQUIPMENT (PSE)

- 6-1. Purpose
- 6-2. PSE Overview
- 6-3. Program Management
- 6-4. Priorities
- 6-5. Risk Analysis
- 6-6. Forecasting Requirements
- 6-7. Coordination
- 6-8. PSE Acquisition
- 6-9. Requests for Non-Army and Non-USAREUR Standard ESSs
- 6-10. Electronic Security Systems

- 6-11. ESS Planning Guidelines
- 6-12. Intrusion Detection Systems
- 6-13. IDS Operating Procedures
- 6-14. IDS Test Procedures
- 6-15. Joint-Services Interior Intrusion Detection System (J-SIIDS)
- 6-16. Alarm Monitoring Group and Integrated Commercial Intrusion Detection Systems
- 6-17. Commercial Intrusion Detection Systems
- 6-18. Closed-Circuit Television (CCTV)
- 6-19. Electronic Entry/Access Control Systems
- 6-20. ESS/IDS Key Control
- 6-21. ESS/IDS Personal Identification Numbers
- 6-22. Physical Security Plans
- 6-23. Maintenance of ESS
- 6-24. Personnel Suitability and Reliability Checks
- 6-25. Movement of ESS Components and Systems
- 6-26. IDS Inspections
- 6-27. Access Rosters
- 6-28. Response to Alarms

CHAPTER 7

USAREUR CONTRACT GUARD PROGRAM

- 7-1. Purpose
- 7-2. Applicability
- 7-3. Objectives
- 7-4. Guard Authority
- 7-5. Types of Guards
- 7-6. Policy
- 7-7. Selection, Qualification, and Security Screening of Guards
- 7-8. Individual Reliability Program
- 7-9. Training
- 7-10. Uniform and Equipment
- 7-11. Establishing and Meeting Requirements
- 7-12. Guard Orders
- 7-13. Contractor Explosive Detector Dogs
- 7-14. Contract Guard Quality Assurance Program

CHAPTER 8

OPM SECURITY OPERATIONS STAFF-ASSISTANCE VISIT PROGRAM

- 8-1. Purpose
- 8-2. References
- 8-3. Security Operations Branch
- 8-4. SAV Schedules
- 8-5. Physical Security SAV
- 8-6. USAREUR Contract Guard SAV
- 8-7. Intention of SAV Program
- 8-8. Required SAV Actions (Physical Security)
- 8-9. Required SAV Actions (Contract Guard Program)
- 8-10. Report Format

CHAPTER 9

SECURITY EQUIPMENT WORKING GROUP (SEWG)

- 9-1. General
- 9-2. Policy
- 9-3. Definition of Nonstandard Equipment
- 9-4. SEWG Responsibilities
- 9-5. Program Management

Appendixes

- A. References
- B. Guidelines for Developing Installation Barrier Plans
- C. Sample Format for Unit Physical Security Standing Operating Procedure
- D. Instructions for Completing AE Form 190-13I
- E. Instructions for Completing AE Form 190-13L

Table

- B-1. Barrier Guidelines

Figures

- 2-1. Sample Restricted Area Sign
- 3-1. Request for Medical-Records Check
- 3-2. Request for Personnel-Records Check
- 3-3. Request for Provost Marshal or Security-Office Records Check
- 3-4. Sample Arms Room Unaccompanied-Access Roster
- 3-5. Appointment Memorandum for Primary or Alternate AA&E Key Custodian
- 3-6. Bilateral Storage Agreement for Consolidated Arms Room
- 3-7. Intrusion Detection System (IDS) Sign
- 3-8. Master Authorization List (MAL)
- 3-9. Monthly Serial Number Inventory Record
- 4-1. ACP Conceptual Functional Layout 1
- 4-2. ACP Conceptual Functional Layout 2
- 4-3. Force Protection ACP Sign
- 4-4. Force Protection ACP Signposts
- 5-1. Appointment Memorandum for Primary or Alternate Administrative Key Custodian
- 6-1. Sample Request for Non-Army or Non-USAREUR Standard ESS
- B-1. Sample Matrixes
- B-2. Sample Drawing Showing Number and Type of Barriers
- B-3. Types of Barriers

Glossary

CHAPTER 1

INTRODUCTION

1-1. PURPOSE

This regulation—

- a. Describes physical security (PS) requirements from regulatory sources.
- b. Prescribes support documentation and records that each unit must maintain.
- c. Is a tool that commanders may use to effectively manage their PS program.

1-2. REFERENCES

Appendix A lists references.

1-3. EXPLANATION OF ABBREVIATIONS

The glossary defines abbreviations.

1-4. RESPONSIBILITIES

Commanders have an inherent PS responsibility for their commands. This responsibility will not be delegated or transferred, except by official orders.

a. Provost Marshal, USAREUR. The Provost Marshal (PM), USAREUR, is the proponent for and will exercise staff supervision over the Army in Europe Physical Security Program. The USAREUR PM will—

(1) Appoint a command physical security officer (PSO) in writing that will determine theater-wide PS requirements and advise subordinate commanders of deficiencies that threaten the security of the U.S. Government and personnel.

(2) Establish a PS program to plan, formulate, and coordinate all PS matters.

(3) Ensure that practical, effective, and common sense measures are used when planning, formulating, and coordinating PS matters.

(4) Serve as the proponent for and the manager of physical security equipment (PSE) in the European theater according to AR 190-13, paragraph 4-7.

(5) Ensure required fiscal resources for security and law enforcement are programmed for in the planning, programming, and budgeting system.

(6) Ensure PS personnel coordinate the design criteria for new construction projects. PS personnel will review all plans and specifications at every step of the planning, design, and construction process.

(7) Establish policy to ensure the procedures outlined in chapter 6 are followed in the issue, purchase, lease, and lease renewal of PSE.

(8) Provide an advisory member (major, GS-12, or above) to the Army Physical Security Equipment Action Group.

(9) Review requests for waivers or exceptions to DA PS requirements, make recommendations, and forward the requests to the HQDA approval authority for final decision.

(10) Review and approve or disapprove requests for waivers or exceptions to PS requirements.

(11) Manage the USAREUR Contract Guard Program and provide technical assistance to commanders on all aspects of security-guard requirements. This will include developing and publishing a standard performance work statement (PWS) for contract-guard services in the European theater.

(12) Nominate for appointment a contracting officer's representative (COR) to manage the daily execution of civilian-guard service contracts that are funded and centrally managed by HQ USAREUR/7A.

(13) Conduct inspections of security-guard programs in the European theater to ensure compliance with USAREUR Contract Guard Program requirements and policy according to this regulation and the USAREUR contract guard PWS.

(14) Establish policy and procedures to ensure arms, ammunition, and explosives (AA&E) are controlled and accounted for at all times.

(15) Establish and implement a security staff-assistance program to evaluate and help commanders execute PS programs.

(16) Manage the High-Risk Personnel (HRP) Program for the Army in Europe.

(17) Manage the Installation Access Control System (IACS) for the Army in Europe.

(18) Conduct command-compliance inspections of PS programs in the European theater to ensure these programs comply with regulatory requirements.

b. G3, USAREUR. The USAREUR G3 will ensure that requests—

(1) To procure electronic security systems (ESSs) for contingency operations and requests for nonstandard force protection/physical security (FP/PS) equipment are coordinated through the USAREUR Security Equipment Working Group (SEWG) and approved by the USAREUR PM.

(2) For ESS funding include all appropriate supporting documentation and approvals required by regulation before approving the funding.

c. Engineering Division, United States Army Installation Management Agency, Europe Region Office (IMA-Europe). The Engineering Division, IMA-Europe, will—

- (1) Coordinate the review of all USAREUR and IMA-Europe level planning documents and construction plans and specifications at all stages of their development with the Office of the Provost Marshal (OPM), HQ USAREUR/7A.
- (2) Ensure installation planning boards include a PS representative from the local provost marshal or security office as a voting member on all actions. These representatives will ensure that provisions of this regulation and other security-related publications are considered during PS planning.
- (3) Develop policy and procedures to ensure that the local PS representative has reviewed every force project request (DA Form 4283) and that PS recommendations are included in the project before final approval or execution.
- (4) Provide intrusion detection system (IDS) and ESS maintenance services by establishing an IMA-Europe-level IDS/ESS installation, training, and maintenance contract to support the USAREUR standard IDSs and ESSs.
- (5) Provide contracting officer representative services to manage and provide oversight for the installation, training, and maintenance contract.

d. G6, USAREUR. The USAREUR G6 will use information provided by base support battalion (BSB) provost marshal offices, identify the number and locations of IDSs, and establish policy and procedures to ensure dedicated communication lines are available to support IDS requirements throughout the European theater.

e. Commanders of USAREUR Major Subordinate and Tenant Commands. Commanders of USAREUR major subordinate and tenant commands will—

- (1) Provide appropriate command emphasis to the Army in Europe Physical Security Program.
- (2) Ensure security programs provide for the safeguarding of personnel, facilities, equipment, operations, and materiel during mobilization and war.
- (3) Ensure a command PSO is appointed in writing.
- (4) Ensure the command PSO has successfully completed formal PS training conducted by the United States Army Military Police School (USAMPS) or has attended a DOD-approved course of instruction.
- (5) Ensure subordinate units and activities that receive “not adequate” ratings on PS inspection reports submit reports of corrective actions within 30 calendar days after the inspection to the inspecting agency or activity.
- (6) Ensure a PS representative is an active participant in the Joint Antiterrorism Working Group (JAWG) process.
- (7) Ensure all elements of their command use and comply with this regulation when executing their PS program.
- (8) Conduct command PS inspections and identify PS requirements of subordinate command activities.
- (9) Review subordinate PS plans annually.
- (10) Ensure PS plans provide for proper protection and security for both Government and personal property left behind when units deploy.
- (11) Ensure resources required for PS are identified to the servicing BSB and area support team (AST).
- (12) Ensure coordination is made with the servicing director of public works (DPW) and PS personnel from the servicing provost marshal office when design criteria for new construction projects is formulated. Also ensure that servicing PS personnel review all plans and specifications at every step of the planning, design, and construction process.
- (13) Ensure coordination is made with the servicing provost marshal office for IDS and monitoring services before any system is procured to ensure that the system is compatible with existing monitoring systems.

(14) In coordination with PS personnel from the servicing provost marshal office, conduct a risk analysis according to DA Pamphlet 190-51 for all facilities (planned and existing) that are designated or likely to be designated as mission-essential vulnerable areas (MEVAs).

(15) Ensure that requirements for IDSs and monitoring services are coordinated with the local provost marshal office and director of information management (DOIM) for monitoring and communication-line support.

f. Commanders of Non-USAREUR Tenant Commands and Activities. Commanders of non-USAREUR tenant commands and activities will—

(1) Ensure PS interests are represented in the JAWG process and other planning processes.

(2) Ensure elements of their command or activity comply with and use this regulation when executing their PS program.

(3) Ensure resources required for PS are identified to the servicing BSB or AST.

(4) Ensure coordination is made with the servicing DPW and PS personnel from the servicing provost marshal office when design criteria for new construction projects are formulated. Also ensure that servicing PS personnel review all plans and specifications at every step of the planning, design, and construction process.

(5) Ensure coordination is made with the servicing provost marshal office for IDSs and monitoring services before any system is procured to ensure that the system is compatible with existing monitoring systems.

(6) Forward requests identifying PS-support requirements for Government-owned, contractor-operated facilities unable to support these requirements to the next higher headquarters or supporting area support group (ASG), BSB, or AST.

(7) Ensure that requirements for IDSs and monitoring services are coordinated with the local provost marshal office and DOIM for monitoring and communication-line support.

g. Commanders of ASGs. ASG commanders are responsible for the PS programs of their communities as directed by the senior tactical commander (STC). ASG commanders will—

(1) Ensure PS programs provide for the safeguarding of personnel, facilities, equipment, operations, and materiel during mobilization and war.

(2) Ensure BSB commanders identify and approve MEVAs in writing and revalidate the consolidated MEVA list each year during the JAWG process.

(3) Ensure an ASG PSO is appointed in writing.

(4) Ensure the ASG PSO has successfully completed formal PS training conducted by the USAMPS or has attended a DOD-approved course of instruction.

(5) Ensure a member of the ASG provost marshal PS section is an active participant in the JAWG process.

(6) Ensure all elements of their command comply with and use this regulation when executing their PS program.

(7) Ensure command inspections and PS staff-assistance visits (SAVs) are conducted to evaluate subordinate command activities, installations, and facilities.

(8) Review subordinate-command PS plans each year.

(9) Synchronize and standardize PS requirements, plans, training, and operations in their area of responsibility (AOR).

(10) Ensure BSB and AST PS plans include provisions for continuing PS protection of unit and personal assets left behind when tenant units deploy.

(11) Ensure resources required for the PS program are identified.

(12) Ensure engineers and PS personnel coordinate with each other when design criteria for new construction projects is formulated. Also ensure that servicing PS personnel review all plans and specifications at every step of the planning, design, and construction process.

(13) Ensure the PSO is properly trained. This includes having attended the Electronic Security Systems and Security Engineering and Design courses sponsored by the United States Army Corps of Engineers (USACE). Information on these courses may be obtained from the Security Operations Branch, OPM (DSN 381-7379/7338).

(14) Ensure subordinate units and activities that receive “not adequate” ratings on PS inspection reports submit reports of corrective actions within 30 calendar days after the inspection to the inspecting agency or activity.

(15) Ensure risk analyses are performed for all facilities (planned and existing) that are designated or likely to be designated as MEVAs.

(16) Ensure PS inspections and surveys are conducted when required by regulation or when directed.

(17) Ensure installation commanders develop, set up, and maintain policy and procedures to control installation access. Commanders will—

(a) Determine the additional degree of control required over personnel and equipment entering or leaving the installation.

(b) Prescribe and distribute procedures for searching people and their possessions on the installation. These procedures will cover searches conducted as people enter the installation, while they are on the installation, and as they leave.

(c) Enforce the removal of, or deny access to, persons who threaten the order, security, or discipline of the installation.

(18) Ensure that requirements for IDSs and monitoring services are coordinated with the local provost marshal office and DOIM for monitoring and communication-line support.

(19) Manage the security guard program for their respective ASG. Commanders will—

(a) Provide for daily supervision and quality control of the contract guard force in their AOR.

(b) Prescribe and distribute procedures to ensure military and civilian personnel advisory center (CPAC) (DA and local-national hire) guard forces are adequately staffed, trained, equipped, and supervised to perform their assigned guard mission.

(c) Ensure locally procured contract security-guard services meet provisions of chapter 7 and the governing USAREUR contract guard PWS.

(d) Appoint the ASG and BSB provost marshals as the commander’s staff proponent for all matters pertaining to contract guard programs at the ASG and BSB level. Likewise, commanders will assign COR and site contracting officer’s representative (SCOR) responsibility to the ASG or BSB provost marshal office, since security-guard services are a military police (MP) functional responsibility. This will create a closer link for planning, executing, and coordinating law-enforcement response operations.

(e) Ensure enough SCORs, quality assurance evaluators (QAEs), or both are appointed to manage and implement quality assurance plans for locally procured contract-guard services and contract-guard services centrally managed and funded by USAREUR (for example, the Germany-wide guards services contract). For contracts centrally managed by USAREUR, the OPM has overall, funding, management, and COR responsibility. The ASG, however, is responsible for the oversight and quality assurance of contract guards assigned to their AORs through locally appointed SCORs and QAEs.

(f) Ensure permanently assigned CORs and SCORs are not given additional duties that could interfere with their ability to provide adequate contract oversight and quality-assurance program management.

(g) Ensure personnel selected for appointment as CORs and SCORs have enough experience and working knowledge of law enforcement and physical security to manage a civilian contract-guard services program.

(h) Identify, validate, and request temporary and permanent contract-guard requirements according to chapter 7.

(i) Monitor the submission of background checks for contract-guard candidates to ensure the required checks in chapter 7 and the governing contract guard PWS are completed to standard.

(j) Validate all contract guard posts annually and submit validations to the OPM, HQ USAREUR/7A (AEAPM-SO), Unit 29931, Bin 153, APO AE 09086-9931 by 1 October each year. Security-guard-services contracts will be modified to terminate any excess requirements reported. If applicable and cost-effective, commanders should consider using ESSs instead of costly contract-guard services.

(k) Conduct periodic command inspections and SAVs to ensure contract-guard quality-assurance plans and requirements are being implemented in accordance with chapter 7 and the governing contract guard PWS.

h. ASG and BSB Provost Marshals. Provost marshals are responsible for managing their command PS program. Provost marshals or PSOs will—

(1) Determine the priority of the MEVA list based on the results of a risk analysis, review the list during the JAWG process, and make final recommendations to the BSB commander concerning installation activities or areas that should be designated as MEVAs.

(2) Assess installation PS needs by conducting PS surveys and inspections.

(3) Recommend PS considerations when preparing installation engineer construction projects, including during the design phase.

(4) Ensure PS considerations are included in new construction, renovation, modification efforts, and lease acquisition.

(5) Serve as the single POC for PSE for units in the AOR of the ASG or BSB commander.

(6) Ensure equipment requirements are coordinated with the user, facility engineer, and communication personnel.

(7) In coordination with local intelligence and law-enforcement agencies, develop an installation threat statement.

(8) Monitor the resource management (funds and personnel) of the ASG or BSB PS program.

(9) In coordination with the ASG or BSB resource management office and the USAREUR PM, plan and program resources needed for PS projects in the program-budget cycle.

(10) Monitor the funding of all PS program resource requirements to ensure the funding is appropriate.

(11) Coordinate PS efforts with the ASG or BSB antiterrorism officer and local DPW.

(12) Coordinate with the local DPW during the planning, design, and construction of all projects to identify PS and antiterrorism requirements, and to ensure that these requirements are incorporated into projects at the start of project planning.

(13) Review planning documents and construction plans and specifications for construction projects at all stages of their development.

(14) Send copies of all PS inspection reports with a “not adequate” rating to the USAREUR PM.

(15) Provide weekly updates to the USAREUR PM on PS issues that are of interest to the USAREUR Command Group.

(16) Keep copies of and monitor all waivers and exceptions to PS requirements for units and activities in their AOR.

(17) Help prepare and review requests for exceptions and waivers to current HQDA and Army in Europe PS policy and procedures.

(18) Establish a PS training program and provide PS training when required.

(19) Ensure PS inspections and surveys are conducted when required by regulation or when directed by the commander.

(20) Develop standard inspection checklists and incorporate them in their training and Security Management System (SMS) program. Checklists may be used as guides. Checklists, however, generally do not cover all requirements.

(21) Serve as the proponent and subject-matter expert to commanders on all aspects of the command security-guard-force program. Also, develop, implement, and manage local security guard programs as directed by higher authorities.

(22) Designate qualified QAE personnel to help SCORs implement contract-guard quality-assurance programs. Commanders should consider using MP supervisory personnel to routinely check contract guard posts to ensure all required guard posts are properly manned, resourced, and operated. The frequency of SCOR and QAE checks will be according to chapter 7.

i. Commanders of Units and Activities. Commanders of units and activities will—

(1) Ensure all elements of their unit or activity comply with and use this regulation when executing their PS program.

(2) Appoint in writing a PSO who will be responsible for the overall PS program.

(3) Develop and publish a unit or organization PS plan.

(4) Coordinate PS plans with their higher headquarters, local security forces, and supporting military intelligence (MI) agencies.

(5) Coordinate PS plans once each year with the BSB provost marshal office to ensure their security procedures are consistent with current requirements and directives.

(6) Maintain a copy of the servicing BSB or AST PS plan. Commanders will direct subordinate units to maintain a copy of the host-organization's PS plan if the units are tenants of a different AST or BSB.

(7) Designate and approve restricted areas and provide this information to the installation commander for FP planning.

(8) Identify to the BSB provost marshal those facilities that are vulnerable to a credible threat and that are essential to the accomplishment of the organization's mission for consideration as a MEVA.

(9) Ensure that agreements governing consolidated AA&E storage facilities clearly define the responsibilities of each unit or activity for the items stored.

(10) Ensure serious incident reports (SIRs) are submitted in a timely manner according to AR 190-40.

(11) Ensure that key custodians have written appointment orders specifying their responsibility to issue and receive keys and maintain accountability for office, unit, or activity keys.

(12) Maintain a key-control register (DA Form 5513-R) at all times to ensure continuous accountability of keys (including reserve sets) for locks used to secure Government property.

(13) Review inspection and survey reports received from inspecting agencies and ensure that corrective actions are taken for reported deficiencies within the timeframes outlined in this regulation.

(14) Maintain key-and-lock inventories using a key-and-lock inventory list or DA Form 5513-R.

(15) Ensure that personnel meet training and certification requirements before they are armed to perform armed-guard duties.

(16) Ensure that deploying personnel are briefed on in-transit security requirements.

(17) Ensure that requirements for IDSs and monitoring services are coordinated with the local provost marshal office and DOIM for monitoring and communication-line support.

j. Commander, 202d Military Police Group. The Commander, 202d Military Police Group, will—

(1) Provide appropriate, threat-related criminal information to provost marshals.

(2) Plan and coordinate personal protective services for DOD and DA officials as directed by HQDA.

(3) Conduct threat assessments for personnel designated as HRP level 1 or as directed by HQDA or the CG, USAREUR/7A.

(4) Establish procedures to ensure appropriate liaison between the United States Army Criminal Investigation Command (USACIDC), the United States Army Intelligence and Security Command, provost marshals, and FP/PS officers operating in support of the USAREUR FP/PS Program.

(5) Immediately notify the affected ASG or BSB provost marshal, the servicing FP/PS officer, and the CG, USAREUR/7A, on receipt of time-sensitive threat information.

(6) Give a copy of USACIDC initial and final reports on terrorist acts to the USAREUR G2, USAREUR G3, and the USAREUR PM.

(7) Immediately provide terrorist-related criminal information to local MI detachments or to the USAREUR G2 and the USAREUR PM.

k. Commander, 66th Military Intelligence Group. The Commander, 66th Military Intelligence Group, will—

(1) Provide appropriate threat-related information to local or affected provost marshals.

(2) Conduct threat assessments for personnel designated as HRP level 1 or as directed by HQDA or the CG, USAREUR/7A.

(3) Establish procedures to ensure appropriate liaison between USACIDC, the United States Army Intelligence and Security Command, provost marshals, and FP/PS officers operating in support of the USAREUR FP/PS Program.

(4) Immediately notify the affected ASG or BSB provost marshal, the servicing FP/PS officer, and the CG, USAREUR/7A, on receipt of time-sensitive threat information.

l. ASG and BSB PSOs. ASG and BSB PSOs will—

(1) Implement their unit PS program.

(2) Validate compliance with all PS regulations, policy, and programs.

(3) Keep the commander informed of PS issues.

(4) Serve as the POC for all unit PS issues and coordinate PS actions.

(5) Serve as the primary POC for all unit PS projects.

(6) Conduct PS inspections and SAVs.

(7) Coordinate PS training for the command.

rating. (8) Monitor the status of corrective actions related to PS inspection and survey reports that receive a “not adequate”

(9) Coordinate with the DPW and other security offices to ensure proper coordination of PS projects.

(10) Prepare the unit PS plan.

(11) Provide input to the unit PS and antiterrorism-funding processes.

(12) Use the SMS to track all inspections, surveys, waivers, and exceptions, and to generate reports.

m. PSOs at USAREUR Major Subordinate and Tenant Commands. PSOs at USAREUR major subordinate and tenant commands will—

(1) Be responsible for implementing their command PS program.

(2) Ensure subordinate units and activities comply with PS requirements.

(3) Serve as the POC and coordinator for PS matters, and respond to ASG requirements when required.

(4) Conduct PS SAVs as needed or directed to determine compliance with regulatory requirements.

(5) Inform their commander and ASG (if applicable) of PS issues.

(6) Monitor corrective actions taken by subordinate units and activities on deficiencies noted on command PS inspection and survey reports.

(7) Identify PS requirements to their higher headquarters, servicing DPW, and BSB provost marshal, as required.

n. Unit and Activity PSOs and PS Noncommissioned Officers (NCOs). Unit and activity PSOs and PS NCOs will—

(1) Write and implement their unit PS plan and security standing operating procedures (SOPs).

(2) Ensure that the unit complies with PS requirements.

(3) Submit and monitor the status of work orders relating to PS and request BSB support to prioritize or accomplish work orders when necessary.

(4) Submit reports of corrective actions taken for deficiencies noted on unit or activity PS inspections and survey reports to the inspecting activity or agency.

(5) Inform and advise the commander on PS matters.

(6) Manage or provide oversight to the unit key-control program.

CHAPTER 2

ARMY IN EUROPE PHYSICAL SECURITY PROGRAM

2-1. GENERAL

a. PS is a critical part of the Army in Europe Force Protection Program. PS measures are designed to detect, deter, delay, and defend against threats to U.S. Forces assets. PS measures are a combination of active or passive systems, devices, and security personnel. Measures may be physical (for example, barriers, fences, lights, walls), electronic (for example, alarms, cameras, electronic entry/access control systems (EECSs)), and procedural (for example, security checks, inspections and surveys, security training and awareness programs, property inventory and accountability procedures). A successful PS program cannot be achieved without appropriate command emphasis and the cooperation of every element of a commander's staff. PS personnel must be fully engaged in and remain active participants in the Army in Europe Force Protection Program.

b. This chapter—

(1) Implements the requirement in AR 190-13 for major Army command (MACOM) commanders to establish a PS program.

(2) Prescribes policy and procedures and assigns responsibility for developing a practical and effective physical security program for the Army in Europe.

2-2. THREAT ASSESSMENT

PS programs must be tailored to meet local needs. A key element of this process is assessing the local threat. Installations and their equivalents will develop a local threat statement. This statement will identify local threats and make full use of investigative resources available in the geographic area to anticipate criminal and intelligence activities that threaten the security of U.S. Forces property and personnel. The PS threat assessment will be taken from the overall FP threat statement. The local threat statement must be included in the installation PS/FP plan.

2-3. LIAISON

As a minimum, liaison will be established with the following agencies:

- a. Local MI field offices.
- b. Local civilian police departments.
- c. Installation criminal investigation division, MI, and MP agencies.

2-4. PHYSICAL SECURITY PLANNING

a. Commanders at all levels must plan for the security of assets under their control. PS plans will tie security measures together and integrate security efforts by assigning responsibilities, establishing procedures, and ensuring subordinate plans complement each other. Plans must include realistic, reasonable, and affordable protective measures. Requirements at different force protection conditions (FPCONs) must be identified.

b. PS planning includes—

(1) Coordinating with installation PS, FP, engineer, and information-management personnel to ensure that all requirements are identified and responsibilities are assigned.

(2) Ensuring that vulnerability assessments and site security surveys are conducted.

(3) Integrating PS into contingency, mobilization, and wartime plans.

(4) Identifying in priority order the resources critical to the performance of the command's mission.

(5) Identifying and establishing minimum PS standards for protecting MEVAs.

(6) Designing ESSs to reduce vulnerability to potential or credible threats, and to reduce vulnerabilities and reliance on fixed security forces.

(7) Training security forces at facilities or sites to defend against and respond to threats to U.S. Forces assets.

(8) Identifying requirements that cannot be met due to a lack of resources or manpower.

(9) Coordinating and maintaining liaison with the host nation and other non-organic or assigned security forces.

(10) Ensuring preplanned reactive measures are established and guidance is provided in writing for the following:

- (a) Bomb threats.
- (b) Civil disturbances.
- (c) Consequence management.

- (d) Increased FPCONs.
- (e) Intrusion or mass-notification alarms.
- (f) Natural disasters.
- (g) Other contingencies that would seriously affect the ability of personnel to perform their mission.

(11) Maintaining barriers that control access to installations or areas.

(12) Pre-designation and pre-positioning of personnel, equipment, and other resources used to enforce restricted access and respond to incidents.

(13) Exercising contingency plans to validate their effectiveness.

2-5. PHYSICAL SECURITY PLAN

a. Commanders will develop and maintain an installation PS plan and include it as an annex to their FP plan. The PS plan will be developed according to AR 190-13, paragraph 2-9, and follow the format and include the content outlined in FM 3-19.30, appendix F. PS plans will be part of the unit antiterrorism/force protection (AT/FP) program and must incorporate elements of a comprehensive PS program (for example, access control, barriers, guard forces, key-and-lock control, lighting). PS plans will include tenant activities, DOD elements, and personnel over which the commander has AT/FP responsibility.

b. The BSB or AST commander is responsible for coordinating PS plans for units and activities in the AOR. PS plans will—

- (1) Assign responsibilities and establish procedures.
- (2) Addresses contingency procedures for when a unit that is assigned a specific task is deployed.
- (3) Address changes in requirements at higher FPCONs.
- (4) Ensure subordinate and tenant activity plans integrate with and complement the installation plan.
- (5) Be reviewed annually.
- (6) Be exercised once every 2 years to evaluate the plan's effectiveness and validity.

c. Appendix B provides guidance on barriers and barrier plans.

2-6. STANDING OPERATING PROCEDURES

SOPs will address unique security requirements and procedures. Unit commanders and heads of activities will approve SOPs. Appendix C provides a sample format for unit PS SOPs.

2-7. MISSION-ESSENTIAL VULNERABLE AREAS

MEVAs consist of equipment, property, and facilities that have been recommended by the BSB provost marshal and approved by the BSB commander as requiring additional protection through the application of increased PS measures, procedures, and equipment.

a. MEVAs are not the same as high-density targets (HDTs) or high-value targets (HVTs). An HDT or HVT, however, may be designated as a MEVA.

b. A facility will be designated as a MEVA when the facility is essential to an installation or organization mission and is vulnerable to a threat that is intent on removing sensitive equipment or property, or on destroying, damaging, or otherwise tampering with equipment or property, including by acts of terrorism. Examples of activities and facilities that should be considered for designation as MEVAs are as follows:

(1) Ammunition and explosives storage rooms, facilities, and depots that store ammunition used for training, deployment, or FP duties.

(2) Arms storage, manufacturing, or rebuilding facilities, and areas critical to supporting units or commands for training, deployment, or FP duties.

(3) Emergency operations centers.

(4) Military-owned or -operated aircraft and aircraft parking and maintenance areas.

(5) Sites and facilities used to store or process classified information.

(6) Critical communications facilities.

(7) Consolidated supply and storage facilities containing sensitive items or equipment and property critical to a unit or organization mission.

(8) Controlled drug and narcotic vaults and other medical-supply storage areas.

(9) Major or critical automated data processing (ADP) facilities.

(10) IDS monitoring stations.

(11) Petroleum, oils, and lubricants (POL) storage and dispensing points critical to unit deployments or operations.

(12) Power-generation and -distribution facilities (alternate and primary) critical to maintaining operations.

(13) Water or food-source facilities critical for sustaining adequate supplies in case of emergency.

c. A risk analysis will be conducted for each MEVA according to DA Pamphlet 190-51. The risk analysis will be conducted by the BSB physical security inspector (PSI) in coordination with the unit or activity commander.

d. The BSB provost marshal will rank MEVAs based on the results of the risk analysis, existing security measures, and threat analysis.

e. The BSB commander will review and approve the MEVA list each year during the JAWG process and send the list to the ASG.

f. ASG provost marshals will consolidate approved MEVA lists and send them to the Chief, Security Operations Branch, OPM, by 1 September each fiscal year.

g. The OPM will send the consolidated MEVA list to the JAWG for review, prioritizing by HQ USAREUR/7A, and approval.

2-8. RISK ANALYSIS

a. DA Pamphlet 190-51 provides the background and explanation of step-by-step procedures for determining security requirements and conducting a risk analysis for categories of Army property.

b. A risk analysis will be conducted on all MEVAs—

(1) When a unit or activity is activated.

(2) When a unit permanently relocates to a new site or facility.

(3) When no formal record exists of a previous risk analysis.

(4) At least every 3 years or more frequently at the discretion of the unit or activity commander.

(5) During the planning stages of new facilities, additions to facilities, and facility renovations.

(6) When an incident occurs in which an asset is compromised.

c. The risk analysis will be conducted by the PSI in coordination with the unit or activity commander.

2-9. RESTRICTED AREAS

A restricted area is an area or facility that is either required by regulation or identified by the commander as requiring additional security and access controls to restrict access to classified information and other DOD assets.

a. Categories of Restricted Areas. USAREUR categorizes restricted areas into three different types, each of which requires a different level of security and access control.

(1) Exclusion Area (Most Secure). An exclusion area is a restricted area containing one of the following:

(a) A security interest or other matter of such nature that access to the area constitutes access to the security interest or matter.

(b) A security interest or other matter of such vital importance that proximity resulting from access to the area is treated equal to (a) above.

(2) Limited Area (Second Most Secure). A limited area is a restricted area containing a security interest or other matter of such nature that uncontrolled movement will permit access to the security interest or matter. Access in limited areas may be controlled by requiring escorts or by other internal restrictions and controls.

(3) Controlled Area (Least Secure). A controlled area is that portion of a restricted area usually near or surrounding an exclusion or limited area. Entry to the controlled area is restricted to authorized personnel. However, movement of authorized personnel in this area is not necessarily controlled. Mere entry to the area does not provide access to the security interest or other matter in the exclusion or limited area. The controlled area is provided for administrative control or safety, or as a buffer zone for security in-depth for the exclusion or limited area. The appropriate commander establishes the degree of control of movement.

b. Designation of Restricted Areas.

(1) When conditions warrant, commanders and heads of organizations will designate restricted areas in writing to protect classified information and safeguard property or material for which they are responsible.

(2) Installation tenant units and activities will provide a list of designated restricted areas to the installation commander for planning purposes.

(3) The designation of restricted areas for activities not on installations will be by the authority of the activity commander or officer in charge.

(4) When required, physical safeguards will be installed to deter unauthorized persons or deny them access to a restricted area.

(5) Commanders designating restricted areas for the protection of classified information will notify the USAREUR G2 (AEAGB-SAD, DSN 370-7574/7088).

c. Posting Restricted Areas.

(1) Except when they would advertise an otherwise concealed area or would conflict with host-nation agreements, signs or notices will be posted in conspicuous and appropriate places to identify restricted areas. This includes signs posted at each entrance or approach to the area and on perimeter fences or boundaries of the area.

(2) Failure to post conspicuous signs and notices to give people approaching a restricted area actual knowledge of the restriction may seriously hamper any resulting criminal prosecution.

(3) Each sign will be gray with black text and include the statement shown in figure 2-1.

RESTRICTED AREA

THIS AREA HAS BEEN DECLARED A RESTRICTED AREA. UNAUTHORIZED ENTRY IS PROHIBITED. ALL PERSONS (AND VEHICLES, if applicable) ENTERING HEREIN ARE LIABLE TO SEARCH. PHOTOGRAPHING OR MAKING NOTES, DRAWINGS, MAPS, OR GRAPHIC REPRESENTATIONS OF THIS AREA OR ITS ACTIVITIES ARE PROHIBITED UNLESS SPECIFICALLY AUTHORIZED BY THE COMMANDER. ANY SUCH MATERIAL FOUND IN THE POSSESSION OF UNAUTHORIZED PERSONS WILL BE CONFISCATED. VIOLATORS WILL BE SUBJECT TO PROSECUTION UNDER APPLICABLE LAWS.

Figure 2-1. Sample Restricted Area Sign

(4) In areas where a language other than English is commonly spoken, warning signs will be in both the local language and English.

c. Procedures for Handling Restricted-Area Violations.

(1) Any person who enters a restricted area without authority will be detained and immediately turned over to MI, MP, or local-national police authorities for questioning.

(a) The person will be searched according to AR 190-30. Any maps, notes, photographs, pictures, sketches, or other material describing the restricted area will be seized.

(b) Persons brought before the proper authority for questioning will be advised of their rights according to AR 190-30, appendix C. Questioning will be conducted without unnecessary delay.

(c) If the person was unaware of the restriction and neither acquired nor intended to acquire knowledge of sensitive or classified information by entering, that person will be warned against reentry and released.

(2) If it appears that the person knowingly entered a restricted area, may have acquired or intended to acquire sensitive or classified information by entering, or may have committed some other offense, the following actions will be taken:

(a) Persons not subject to the Uniform Code of Military Justice (UCMJ) will be detained and questioned by MI and MP officials, then turned over to civilian law-enforcement officials. The agency to which the person is transferred will be given a written statement of the facts, the names and addresses of the witnesses, and pertinent exhibits if available.

(b) Persons subject to the UCMJ will be turned over to MI and MP officials.

(3) Facts regarding a deliberate violation of a restricted area will be immediately reported to MI and MP officials.

2-10. PHYSICAL SECURITY SURVEYS

PS surveys are formal, recorded assessments of an installation PS program.

a. PS surveys will be conducted in conjunction with the FP vulnerability assessment to prevent duplication of effort.

b. PS surveys in general must be conducted at least every 3 years.

c. A PS survey is required every 18 months for installations that—

(1) Store nuclear or chemical munitions.

(2) Store conventional AA&E.

(3) Have critically sensitive, multiple-customer ADP service-center activities or facilities.

d. A PS survey is required every 2 years for installations that have highly sensitive, sensitive, or non-sensitive ADP service-center activities or facilities servicing multiple customers.

e. A facility or activity may be surveyed more frequently than described above at the discretion of the ASG or BSB commander.

f. PS surveys should—

(1) Provide the commander an assessment of the overall security posture of the installation.

(2) State in priority order recommended actions that should be taken to reduce vulnerabilities.

(3) Include photographs, sketches, graphs, charts, or site references that would help clarify findings and recommendations, and an assessment of their criticality and vulnerability.

g. DA Form 2806-R will be used to record the findings and recommendations of the survey.

h. The survey report, including exhibits, will be kept on file at the BSB provost marshal office and copies will be forwarded to the—

(1) Installation commander for information and corrective action.

(2) Installation FP officer for information and planning purposes.

(3) ASG commander, provost marshal, and FP officer for information and planning purposes.

i. When deficiencies or vulnerabilities are identified, BSB commanders will provide the ASG commander a report of corrective actions taken to correct deficiencies or reduce vulnerabilities.

j. ASG commanders will establish procedures for following up on reports of corrective actions for deficiencies and vulnerabilities noted on survey reports.

k. Before conducting command inspections, FP vulnerability assessments, pre-joint services integrated vulnerability assessment (JSIVA) assistance visits, and other security assessments and surveys, surveyors or inspectors will request a copy of the most recent PS survey to use during their assessment or survey. Having a copy of the most recent survey provides the surveyor or inspector with historical data used to identify recurring deficiencies.

l. Commanders will program resources to correct deficiencies noted during surveys.

m. Results of an installation PS survey will be used to develop PS projects and a resource plan with the recommended prioritized allocation of resources.

2-11. PHYSICAL SECURITY INSPECTIONS

PS inspections are formal, recorded assessments of PS procedures and measures implemented by a unit or activity to protect its assets. Normally, these inspections are limited to units and activities designated by the commander as MEVAs.

a. PS inspections will be conducted according to AR 190-13, paragraph 2-11; and this regulation.

b. PSIs will not engage in illegal or dangerous conduct to demonstrate security deficiencies or weaknesses observed during an inspection.

c. Inspections may be unannounced. However, before conducting an unannounced inspection, PSIs should review unit-training schedules to ensure that the inspection will not interfere with training.

d. PS inspections will be conducted—

(1) When a MEVA, unit, or activity is activated.

(2) When no record exists of a prior PS inspection.

(3) When a unit or activity changes in a way that may affect existing PS plans and there is an indication or a report of significant or recurring criminal activity.

(4) Every 18 months for conventional-arms and ammunition-storage activities.

(5) Every 18 months for critically sensitive, multiple-customer ADP service-center activities or facilities.

(6) Every 2 years for MEVAs other than those in (4) and (5) above.

(7) For other activities as directed by the local commander.

(8) Every 2 years for highly sensitive, sensitive, or non-sensitive ADP service-center activities or facilities servicing multiple customers. Inspections of all other ADP activities or facilities not classified as critically sensitive will be incorporated into scheduled PS inspections of the individual activity of facility.

(9) If the commander determines that inspections should be conducted more frequently.

e. Courtesy inspections will not be conducted in place of inspections required by regulation.

f. To discourage last-minute cancellations and schedule changes due to lack of preparation, requests to change the date of a scheduled inspection must be approved by the organization's next-higher commander.

g. PSIs will be granted access to U.S. Forces facilities, records, and information on a need-to-know basis consistent with the PSI's clearance for access to classified information and the provisions of applicable regulations.

h. PSIs will give units and activities a verbal out briefing at the completion of the inspection that identifies deficiencies found.

i. Deficiencies noted during the inspection may be correctable on-site during the inspection. Recurring findings will be reported on future PS inspections until the deficiency is corrected.

j. When a deficiency is identified, the unit or activity commander will correct it immediately or use adequate compensatory measures until the deficiency can be corrected. Commanders will use compensatory measures for structural deficiencies pending completion of any work order request. The submission of work order requests alone is not considered a compensatory measure.

k. Deficiencies that are beyond the capability of the local commander to correct because of a lack of resources will be reported to the next-higher commander with a request for resource assistance and a justification and impact statement.

l. DA Form 2806-1-R, the SMS, or both will be used to prepare and record all PS inspections. Attachments may be added to the printed report to clarify unique command requirements.

m. Copies of PS inspection reports will be provided to the—

(1) Commander of the unit or director of the organization inspected.

(2) Commander or director at the next-higher level above the organization inspected.

(3) Installation PSO.

n. Units and activities must keep inspection reports until the next inspection is complete.

o. Provost marshals will send by e-mail the completed inspection report to the inspected unit within 5 workdays after the inspection and send a paper copy within 15 workdays after the inspection.

p. If a unit or activity receives two "not adequate" ratings in a row, the inspecting agency will forward a copy of the report to the OPM, HQ USAREUR/7A (AEAPM-SO), Unit 29931, Bin 153, APO AE 09086-9931.

2-12. REPORTS OF CORRECTIVE ACTION

- a. Units or activities storing AA&E and other sensitive items that receive a “not adequate” rating on a PS inspection will submit a report of corrective action to the inspecting activity and the inspected unit’s higher headquarters within 30 days after the inspection.
- b. The report of corrective action must identify corrective actions taken, compensatory measures implemented, or both to address findings on the survey, inspection, or vulnerability assessment.

2-13. REPORT CLASSIFICATION

The results of a survey, inspection, or assessment often identify critical deficiencies or vulnerabilities in an installation or facility PS program.

- a. According to AR 190-13, paragraph 2-13, reports of completed inspections or surveys will be classified and safeguarded according to DOD 5200.1-R, AR 380-5, and USAREUR Supplement 1 to AR 380-5, as appropriate.
- b. As a minimum, reports will be marked “UNCLASSIFIED/FOR OFFICIAL USE ONLY.”

2-14. WAIVERS AND EXCEPTIONS

- a. Requests for waivers and exceptions to PS requirements will be—
 - (1) Coordinated through the servicing BSB provost marshal office and with the BSB DPW when requesting a waiver or exception in reference to structural deficiencies.
 - (2) Forwarded through the servicing BSB and ASG provost marshal office to the OPM, HQ USAREUR/7A (AEAPM-SO), Unit 29931, Bin 153, APO AE 09086-9931.
 - (3) Submitted in standard memorandum format with AE Form 190-13L. AE Form 190-13L will provide complete justification and state the compensatory measures that are in effect. Appendix D provides information on completing AE Form 190-13L.
- b. Waivers for longer than 12 months will not be granted. One-time extensions may be granted on written request, if justified.
- c. Exceptions will be permanent but must be revalidated every 2 years by HQDA or HQ USAREUR/7A, as appropriate.
- d. When compensatory measures associated with a waiver or exception change or are no longer required, a request for re-determination or cancellation must be submitted.

2-15. SECURITY ENGINEERING SURVEYS

A security engineering survey is the process of identifying through an on-site survey the engineering requirements associated with facility enhancements for PS and antiterrorism, including IDS installation. Security engineering surveys should be performed when planning new construction, renovations, or upgrades to existing facilities where there are likely to be PS requirements. Security engineering surveys may also be requested by the local provost marshal or equivalent security officer to evaluate existing security.

- a. The scope of a security engineering survey is to—
 - (1) Identify assets to be protected.
 - (2) Identify threats to the assets and the levels of protection to which the assets should be protected against them.
 - (3) Identify protective measures, including IDS, which can be used to reduce the vulnerability of the assets to the threats.
 - (4) Determine the cost of proposed protective measures.

b. As a minimum, the following personnel or their representatives should participate in or provide input to the security engineering survey:

(1) The BSB provost marshal or equivalent security officer, including a PS representative.

(2) The DPW. The DPW can help complete the site survey if required, identify site-preparation requirements and associated costs, coordinate follow-on maintenance, and forecast associated maintenance-funding requirements.

(3) A DOIM representative. The DOIM must be requested in writing to identify available communication media and coordinate systems communication requirements.

(4) The director of logistics (DOL). The DOL must be requested in writing to provide assistance with equipment procurement and property book accountability.

(5) The local safety officer and fire marshal (required when planning to install an EECS).

(6) The facility user.

c. Requests for security engineering surveys beyond local capabilities will be sent to the OPM, HQ USAREUR/7A (AEAPM-SO), Unit 29931, Bin 153, APO AE 09086-9931.

d. Technical assistance regarding site surveys, contracts, and the design, installation, and maintenance of IDSs may also be obtained from the Chief of Engineers (COE), Huntsville Center of Expertise for Intrusion Detection Systems (IDS-MCX), Huntsville, Alabama; or from the Program Manager - Physical Security Equipment (PM-PSE), Fort Belvoir, VA. Requests for assistance from the COE or the PM-PSE will be routed through the OPM.

2-16. NEW CONSTRUCTION AND MAJOR RENOVATIONS

Commanders must ensure that every aspect of PS structural design is incorporated into the initial planning or renovation of facilities. PSOs are required to review and authenticate all copies of DD Form 1391 certifying that PS considerations have been thoroughly reviewed and are integrated into the proposed construction as applicable. The PSO will maintain close liaison with installation engineers for early coordination of proposed new construction projects. The PSO should be an active voting member on the installation planning board.

2-17. PHYSICAL SECURITY PERSONNEL

a. The provost marshal, security officer, or commander, as appropriate, will appoint a PSO in writing. The PSO will be responsible for executing and managing the command PS program.

b. Persons being considered for appointment as a PSO must—

(1) Be a first lieutenant, GS-09, or above.

(2) Have at least 2 years left on assignment.

(3) Have experience in managing PS programs.

(4) Have successfully completed formal PS training conducted by the USAMPS or have attended a DOD-approved course of instruction.

(5) Have a current U.S. Secret or higher security clearance.

(6) Be free of any disqualifying criteria according to AR 190-13, paragraph 3-3b.

(7) Have a favorable crime records check (CRC).

c. The provost marshal, security officer, or commander, as appropriate, may hire or appoint a PS specialist, PSI, or PS NCO to support the command PS program. The PS specialist, PSI, or PS NCO provides direct support to the command PSO by executing assigned PS tasks.

d. Persons hired or appointed as a PS specialist, PSI, or PS NCO must—

(1) Be a staff sergeant (may be waived to sergeant), GS-07, or above.

(2) Be provided the opportunity to attend and successfully complete formal PS training conducted by the USAMPS or a DOD-approved course of instruction within 1 year after the initial appointment.

(3) Have at least 2 years left on assignment.

(4) Have a current U.S. Secret or higher security clearance.

(5) Be free of any disqualifying criteria according to AR 190-13, paragraph 3-3b.

(6) Have a favorable CRC.

e. Civilians hired for PSO, PS specialist, and PSI positions must meet the current Office of Personnel Management GS-080 PS qualification standards (<http://www.opm.gov/qualifications/sec-iii/a/0000-ndx.htm>) for the particular grade assigned to the position.

f. Commanders will initiate actions to remove the additional skill identifier (ASI) H-3 from official records of soldiers when the soldier is no longer assigned to a PS position performing PS duties. Commander may restore ASI H-3 to a qualified soldier with the rank of sergeant or staff sergeant at any time according to AR 190-13, paragraph 3-3a.

2-18. PHYSICAL SECURITY TRAINING

Having the appropriate level of training and knowledge is critical to ensure commanders are provided appropriate and timely security guidance.

a. Personnel serving as command PSOs or PSIs must be formally trained in both PS and AT/FP.

(1) The PS training requirement may be met by attending one of the following:

(a) The 2-week Conventional Physical Security Course conducted by the USAMPS.

(b) A DOD-approved course of instruction.

(2) Antiterrorism training can be obtained by attending the Antiterrorism Officers Course conducted by the USAMPS.

b. The Seventh Army Training Command will establish a 1-week, compressed PSO training course in coordination with the OPM, and conduct the course once each quarter. The target audience for this course will be unit-level PSOs and NCOs.

c. ASG and BSB PSOs should have additional training or knowledge in the following areas:

(1) Communications security.

(2) ESS design.

(3) Industrial security.

(4) Information security.

(5) Personnel security.

(6) The resource management, programming, budgeting, and execution system.

(7) Security engineering and design.

2-19. PHYSICAL SECURITY CREDENTIALS

- a. The only authorized credentials for PSOs and PSIs are DA Form 4261 and DA Form 4261-1. Reproductions of these credentials or use of locally produced credentials is prohibited.
- b. USAREUR major subordinate and tenant commands and ASGs may request blank credentials by sending a memorandum to the OPM, HQ USAREUR/7A (AEAPM-SO), Unit 29931, Bin 153, APO AE 09086-9931. The request must identify the quantity required and include a current inventory report identifying the status of previously issued credentials.
- c. PSO and PSI candidates will not be issued credentials, signed up for a PS training program, or awarded the ASI H-3 until a favorable CRC is received.
- d. Commanders will ensure a PS credential custodian is appointed in writing by the provost marshal or security officer. PS credential custodians will—
 - (1) Maintain control and accountability of credentials at all times.
 - (2) Issue credentials using DA Form 410.
 - (3) Establish and maintain an electronic control log to record the issue, withdrawal, disposition, and destruction of credentials. The electronic log will include the following fields for each credential:
 - (a) Credential serial number.
 - (b) Date issued.
 - (c) The following information on the person who received the credential:
 1. Last name.
 2. First name.
 3. Middle initial.
 4. Rank/grade.
 5. Social security number.
 6. Unit assigned.
 - (d) Expiration date. This date will not be later than the date eligible to return from overseas (DEROS), expiration term of service (ETS) date, or 48 months, whichever is sooner.
 - (e) Date withdrawn.
 - (f) Reason withdrawn (for example, permanent change of station (PCS), ETS, person under investigation).
 - (g) Disposition (for example, active, lost, stolen, destroyed).

NOTE: Enter “Pending Issue” in the *Last Name* field of the control log if a credential has not been issued.

- (4) Conduct a quarterly credential inventory and forward the results in writing with an updated copy of the electronic control log to the USAREUR PM by the last day of each quarter.

e. Credentials will—

- (1) Be issued only to qualified USAREUR major subordinate and tenant command, ASG, and BSB PSOs and PSIs.
- (2) Be issued directly to authorized individuals by the PS credential custodian.

- (3) Be completed with the name, rank or grade, physical description, date of birth, social security number, photograph, and signature of the person to whom they are issued.
- (4) Be signed by the provost marshal, security officer, or commander.
- (5) Be laminated by the PS credential custodian. Credentials that have not been laminated are not valid.
- (6) Be carried by the PSO or PSI while conducting inspections or surveys and secured when not in use.
- (7) Be provided double-barrier protection.
- (8) Expire on the recipient's DEROS or ETS date, or 48 months after the date of issue, whichever is sooner.
- (9) Be withdrawn on the recipient's PCS, ETS, or reassignment from the PS position.
- (10) Be withdrawn for cause according to AR 190-13, paragraph 3-3b.
- (11) Be withdrawn if a PSO or PSI is being investigated for criminal or other inappropriate behavior.
- (12) Not be altered in any way.

CHAPTER 3

SECURITY OF ARMS, AMMUNITION, AND EXPLOSIVES (AA&E)

3-1. PURPOSE

This chapter—

- a. Is intended to help unit and activity armorers meet regulatory requirements for arms-room security and accountability.
- b. Is not intended to be a substitute for AR 190-11.
- c. Only applies to man-portable arms and shoulder-fired missiles and rockets. AR 190-11 and chapter 5 of this regulation provide information on bulk-storage requirements.

3-2. GENERAL

- a. Commanders must authorize in writing the storage of sensitive and high-value items (for example, binoculars, expended light anti-tank weapons (LAWs), global positioning systems, night-vision devices, trainers) in an arms room. These items will be inventoried and maintained separately from AA&E.
- b. The term “armed guard” used throughout this chapter is defined as guard personnel having a weapon with a magazine loaded with ammunition inserted into the weapon without a round chambered.
- c. This chapter provides the minimum security requirements for categories of AA&E. Commanders will refer to both Army and Army in Europe safety regulations for guidance on how to obtain an ammunition and explosives storage license for their storage structures and to determine the maximum permissible amount of ammunition and explosives that may be stored.

3-3. CATEGORIES OF AA&E

The minimum-security requirements for AA&E are based on the security risk category of the items. The four security risk categories are as follows:

a. Arms.

(1) Category I: Missiles and rockets. This category—

- (a) Includes non-nuclear man-portable missiles and rockets in a ready-to-fire configuration (for example, Javelin, Stinger, Dragon, LAW, shoulder-launched multipurpose assault weapon (SMAW-D), and AT-4 anti-tank weapon).

(b) Also applies in situations where the launcher tube and the explosive rounds, though not in a “ready-to-fire” configuration, are jointly stored or transported.

(2) Category II: Arms. This category includes light automatic weapons up to and including .50 caliber (for example, M16A2 rifles, squad automatic weapons (SAWs), M-240 machineguns, and 40-millimeter (mm) MK-19 machineguns).

(3) Category III: Arms. This category includes—

(a) Launch tubes and grip stocks for Stinger missiles.

(b) Launch tubes, sight assemblies, and grip stocks for Stinger, Javelin, and SMAW-D missiles.

(c) Trackers for Dragon missiles.

(d) Mortar tubes up to and including 81mm.

(e) Grenade launchers.

(f) Rocket and missile launchers (unpacked weight of 100 pounds or less each).

(g) Flame-throwers

(h) Launcher and missile-guidance sets and the optical sights for tube-launched, optically tracked, wire-guided (TOW) missiles.

(i) Launch-control units for Javelin missiles.

(4) Category IV: Arms. This category includes—

(a) Shoulder-fired weapons other than man-portable missiles, rockets, and grenade launchers that are not fully automatic.

(b) Handguns.

(c) Recoilless rifles up to and including 90mm.

b. Ammunition and Explosives.

(1) Category I. This category includes explosive rounds for category I missiles and rockets.

(2) Category II. This category includes—

(a) Hand or rifle grenades, high explosives, and white phosphorus.

(b) Mines, anti-tank or anti-personnel (unpacked weight of 50 pounds or less each).

(c) Explosives used in demolition operations, such as C-4, military dynamite, and trinitrotoluene (TNT).

(3) Category III. This category includes—

(a) Ammunition, .50 caliber and larger, with explosive-filled projectile (unpacked weight of 100 pounds or less each).

(b) Grenades, incendiary grenades, and fuses for high-explosive grenades.

(c) Blasting caps.

(d) Supplementary charges (uninstalled or installed in projectiles in a manner allowing easy removal without special tools or equipment).

(e) Bulk explosives.

(f) Detonating cords.

(4) Category IV. This category includes—

(a) Ammunition with non-explosive projectiles (unpacked weight of 100 pounds or less each).

(b) Fuses, except for those in (3)(b) above.

(c) Illumination or smoke grenades and teargas (ortho-chlorobenzal malononitrile (CS) and chloroacetophenone (CN)).

(d) Incendiary destroyers.

(e) Riot-control agents (100-pound package or less).

3-4. NONSENSITIVE AA&E

AA&E that does not meet the criteria in this chapter for sensitive items must be safeguarded from pilferage, theft, and wrongful destruction when stored or deployed in the field. As a minimum, non-sensitive AA&E will be provided double-barrier protection when not in use. AR 190-51, chapter 5, provides supplemental minimum-security standards for safeguarding unclassified and non-sensitive Army property.

3-5. STORAGE FACILITIES

a. AA&E will be stored only in facilities that meet the construction standards specified in AR 190-11.

b. Qualified engineer personnel will verify the structural composition of the arms room (for example, walls, ceiling, doors, windows, floor) and arms-storage racks or containers on DA Form 4604-R.

c. The DA Form 4604-R—

(1) Will clearly indicate the highest category of AA&E the facility may store and the date of applicable regulations.

(2) Will be posted in the arms room.

(3) Must be reviewed by the local DPW during inspections and revalidated every 5 years or when a change in construction or category of AA&E occurs.

d. Commanders are authorized 10-percent deviation from the PS construction standards established by this regulation for existing facilities. The percentage of deviation is measured by adding the total percentage for each deviation.

3-6. DETERMINATION OF RELIABILITY

a. Commanders will be selective in assigning personnel to duties involving control of AA&E. Only personnel who are mature, stable, and have shown a willingness and capability to perform assigned tasks in a dependable manner will be assigned to duties that involve responsibility for the control, accountability, and shipment of AA&E.

b. Unit and activity commanders will conduct command-oriented security screenings and background checks according to AR 190-11, paragraph 2-11, to determine the reliability of personnel assigned duties involving the control of AA&E before they are assigned these duties.

c. The following groups of personnel must be screened:

(1) Personnel authorized unaccompanied access to the arms room.

(2) Personnel authorized to receive, store, or issue AA&E at the facility.

(3) Personnel authorized to issue or control keys for AA&E storage facilities.

d. DA Form 7281-R will be used to record screening results and include as a minimum—

(1) A personal interview of the individual by the commander or supervisor.

(2) A request for a medical-records check if the person is active-duty military (fig 3-1). Medical records of civilians may not be checked.

(3) A personnel-records check for military, DOD civilian, and local national employees (fig 3-2).

(4) A provost marshal and security-office records check (fig 3-3).

(5) A records check by the local civilian police in the area of the person's residence if permitted by the host country or local laws.

e. Completed forms will be kept on file in the command until the individual leaves or is relieved of his or her AA&E duties.

f. Security screening will be repeated every 3 years.

g. Unit and activity commanders will program operational funds to cover the cost for recurring local civilian police checks.

h. The following conduct or impairment is just cause to deny access to or appointment of an individual to a duty or position in control of AA&E:

(1) Alcohol abuse.

(2) Unauthorized use, sale, or possession of drugs or narcotics.

(3) A history of mental instability or disorders.

(4) A record of judicial or nonjudicial punishment.

(5) A pattern of behavior or actions that indicate a contemptuous attitude toward the law.

(6) Other character traits, record of conduct, or adverse information that, in the commander's judgment, make the individual's reliability or trustworthiness questionable.

i. Commanders must handle with the utmost discretion any derogatory information received from record checks.

(1) Records of derogatory information will be destroyed unless the commander decides to grant the individual access to the arms room.

(2) Under no circumstances will derogatory information be shared with anyone other than the commander concerned and security officials. Commanders will take appropriate measures to safeguard this information at all times according to Privacy Act requirements.

3-7. ACCESS CONTROL

a. Commanders will ensure that access to AA&E is controlled at all times.

b. Arms-storage facilities will be designated and posted as restricted areas.

c. Routine and unaccompanied access to arms-storage facilities will be limited to the least number of responsible persons designated by the unit or activity commander or manager.

d. Personnel will be granted unaccompanied access only after they have undergone a background check and have a completed DA Form 7281-R. Only the unit or activity commander or manager may authorize unaccompanied access to AA&E.

OFFICE SYMBOL

Date

MEMORANDUM FOR (*address of the organization that maintains copies of the individual's military medical records*)

SUBJECT: Request for Military Medical Records Check, (*individual's name, rank or grade, SSN*)

1. (*Individual's rank or grade, name, SSN, unit*) is being considered for a position requiring unaccompanied access to our unit arms room. AR 190-11, paragraph 2-11, requires a medical-records check on each individual being considered for such a position.
2. Request you review (*individual's rank or grade and name*) medical records and identify any information that may or should be considered when determining his/her suitability for this position.
3. Request you advise me in writing of the results of your records check.
4. The POC is (*rank or grade and name of security officer*), DSN (*telephone number*).

*Unit/Activity Commander
Signature Block*

Figure 3-1. Request for Medical-Records Check

OFFICE SYMBOL

Date

MEMORANDUM FOR (*address of the organization that maintains copies of the individual's personnel records*)

SUBJECT: Request for Personnel Records Check, (*individual's name, rank or grade, SSN*)

1. (*Individual's rank or grade, name, SSN, unit*) is being considered for a position requiring unaccompanied access to our unit arms room. AR 190-11, paragraph 2-11, requires a personnel-records check on each individual being considered for such a position.
2. Request you review (*individual's rank or grade and name*) personnel records and identify any information that may or should be considered when determining his/her suitability for this position.
3. Request you advise me in writing of the results of your records check.
4. The POC is (*rank or grade and name of security officer*), DSN (*telephone number*).

*Unit/Activity Commander
Signature Block*

Figure 3-2. Request for Personnel-Records Check

MEMORANDUM FOR (*Address of BSB provost marshal or security office*)

SUBJECT: Request for (*Provost Marshal or Security-Office*) Records Check, (*individual's name, rank or grade, and SSN*)

1. (*Individual's rank or grade, name, SSN, unit*) is being considered for a position requiring unaccompanied access to our unit arms room. AR 190-11, paragraph 2-11, requires records checks on each individual being considered for such a position.
2. Request your office review your police files to determine if any record is present that may preclude this person from holding such a position.
3. Request you advise me in writing of the results of your records check.
4. The POC is (*rank or grade and name of security officer*), DSN (*telephone number*).

Unit/Activity Commander
Signature Block

Figure 3-3. Request for Provost Marshal or Security-Office Records Check

e. The names and duty positions of authorized personnel will be posted on an unaccompanied-access roster (fig 3-4) inside the arms room and covered from view.

f. Commanders will establish and use the two-person rule for all category I AA&E storage facilities and require that two authorized persons be present during any operation that requires access to category I facilities. Commanders will establish appropriate key-and-lock control procedures to avoid defeating the concept of the two-person rule.

g. The use of the two-person rule for other categories of AA&E is at the discretion of the commander.

NOTE: Commanders will minimize the number of individuals' authorized unaccompanied access. Personnel must be selected based on a genuine need for unaccompanied access to the room. Everyone selected must undergo required background checks and security screening to ensure suitability before granting unaccompanied access.

3-8. KEY-AND-LOCK CONTROLS

a. Only approved locks and locking devices (including hasps and chains) will be used.

b. Commanders will appoint a key custodian in writing (fig 3-5). Only the commander and the key custodian (or alternate, if appointed) may issue keys to, and receive keys from, individuals on the key-access roster.

c. Key custodians will—

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Arms Room Unaccompanied-Access Roster

1. The following individuals are authorized unaccompanied access to this arms room:

NAME	RANK	SSN	UNIT	POSITION
Johnson, Samuel G.	1LT	276-33-7288	289th ENGR CO	Unit Supply Officer
Jones, Pamela M.	SGT	274-22-7690	289th ENGR CO	Unit Armorer
McKinney, John K.	SFC	256-33-3436	343d PSB	Unit Supply NCOIC
Ball, Pamela	SGT	006-55-9122	343d PSB	Unit Armorer

2. Inspecting officers and other visitors will not be allowed unaccompanied access to this arms room unless accompanied by one of the individuals above.
3. The POC is 1LT Johnson, DSN 123-4567.

*Host Unit/Activity Commander
Signature Block*

DISTRIBUTION:

- 1-Tenant Unit/Activity Commander
- 1-Each Individual Concerned
- 1-Posted Inside Arms Room
- 1-Unit Physical Security Officer/NCO
- 1-Physical Security Files

Figure 3-4. Sample Arms Room Unaccompanied-Access Roster

(1) Maintain a record to identify each key and lock and combinations to locks used by the activity, including replacement and reserve keys and locks. This record will show the current location and custody of each key and lock.

(2) Maintain a current roster signed by the commander of persons authorized access to AA&E keys and protect the roster from view. Personnel listed on the key-access roster may transfer custody in writing among themselves. At no time will keys be in the custody of a person not listed on the roster.

MEMORANDUM FOR RECORD

SUBJECT: Duty Appointment for (*Primary or Alternate*) AA&E Key Custodian

1. EFFECTIVE: (*date, grade, name, SSN*) is appointed as the (*Primary or Alternate*) AA&E Key Custodian for the (*unit or activity*) arms room and intrusion detection system (IDS) keys.
2. AUTHORITY: AR 190-11, paragraph 3-8.
3. PURPOSE: Assure proper control, accountability, and handling of keys and locks for the arms room.
4. PERIOD: Until officially relieved or released from this appointment.
5. SPECIAL INSTRUCTIONS: Become familiar with the key-control provisions of AR 190-11.
6. POC: (*rank or grade and name*), DSN (*telephone number*).

Unit/Activity Commander
Signature Block

DISTRIBUTION:

1-Unit/Activity Commander
1-Individual Concerned
1-Unit Physical Security Officer/NCO
1-Physical Security Files

Figure 3-5. Appointment Memorandum for Primary or Alternate AA&E Key Custodian

(3) Maintain DA Form 5513-R at the unit level to ensure continuous accountability for keys. Completed forms will be kept on file for at least 180 days and then disposed of by shredding with a crosscut shredder. The DA Form 5513-R will include the following:

- (a) The printed name and signature of the individual to whom the key is issued.
- (b) The date and hour of issue.
- (c) The serial number of the key or other identifying information.
- (d) The printed name and signature of the person issuing the key.
- (e) The date and hour the key is returned.

(f) The printed name and signature of the individual receiving the returned key.

(4) Inventory keys and padlocks by serial number twice a year. Inventory records must be kept in unit files for at least 1 year and then disposed of by crosscut shredding. A crosscut shredder must be used because the inventory identifies the location of and keys for secure areas. (Having this information could provide quicker access to an area.) The inventory will include a record of keys, locks, key serial numbers, lock serial numbers, lock locations, and the number of keys maintained for each lock. The inventory record will be secured in the key depository.

(5) Sign out keys to authorized personnel only on a DA Form 5513-R. This form may be downloaded from the Army in Europe Publishing System (<https://aepubs.army.mil/ae/public/main.asp>). When not in use, DA Form 5513-R will be kept in a locked container that does not contain and is not used to store classified documents or material and to which access is controlled.

(6) Ensure keys and combinations to locks for AA&E storage facilities, arms racks, IDSs (operational or maintenance), and key containers are not removed from the installation except to provide for protected storage elsewhere.

(7) Ensure keys to AA&E storage buildings, rooms, racks, containers, and IDSs are maintained separately from other keys and are accessible only to those individuals whose official duties require access to them.

(8) Ensure keys required for maintenance and repair of IDSs, including keys to the control unit door and monitor cabinet, are kept separate from other operational IDS keys, and that only authorized maintenance personnel are given access to them.

(9) Ensure that keys for AA&E and IDSs are not stored in containers containing or used to store classified documents or material.

(10) Store the alternate or spare set of AA&E keys in a separate security container that is approved by the General Services Administration (GSA) and that does not contain and is not used to store classified documents or material. The container storing these keys must be located in a different room away from the primary set of keys, and may be stored locally with another unit or organization. If stored outside the unit or organization, a memorandum of understanding with the unit or organization maintaining the keys must be established. A DA Form 5513-R identifying the personnel authorized to sign for the keys must be provided.

(11) Ensure that combinations to safes and security containers are recorded on SF 700, sealed in the envelope provided, and stored in an approved security container according to AR 380-5 and USAREUR Supplement 1.

(12) Ensure that keys to locks securing key containers are given double-barrier physical protection. Also ensure that replacement and reserve locks, cores, and keys are inventoried and secured to prevent access by unauthorized individuals.

d. When not in use, keys will be stored in one of the following:

(1) A container of at least 20-gauge steel or material of equivalent strength that is equipped with GSA-approved, low- (secondary) security padlocks or GSA-approved, built-in, three-position, changeable combination locks.

(2) A class 5 or class 6, GSA-approved, three-position, changeable combination container.

NOTE: These containers must not contain or be used to store classified documents or material.

e. Keys to AA&E storage buildings, rooms, racks, containers, and IDSs may be secured together in the same key container. IDS keys must be secured on a separate key ring from all other AA&E keys.

f. When arms and ammunition are stored in the same areas, keys to those storage areas may be maintained together, but must be kept separate from other keys that do not pertain to AA&E storage.

g. Key containers weighing less than 500 pounds will be fastened to the structure with bolts or chains equipped with secondary padlocks to prevent easy removal.

h. If a key is lost, misplaced, or stolen—

(1) An investigation will be conducted immediately.

(2) The affected locks or cores to locks will be replaced immediately.

(3) A 100-percent serial number inventory will be conducted to determine if any AA&E is missing.

i. The use of a master key or multiple-key system is prohibited.

j. Padlocks will be locked to the staple or hasp when the area or container is open to prevent theft, loss, or substitution of the lock. Padlocks and keys that do not have a serial number will be given one. This number will be inscribed on the lock or key as appropriate.

k. When individuals are charged with the responsibility for safeguarding or otherwise having keys immediately available, they will sign for a sealed container of keys on DA Form 2062.

(1) A “sealed container” is a locked and sealed key container or a sealed envelope containing the key or combination to the key container. When a sealed container of keys is transferred from one individual to another, the unbroken seal is evidence that the keys have not been disturbed. The seal need not be broken to inventory the keys. The commander, however, may require an inventory when a sealed key container is transferred. The keys must be inventoried if evidence of tampering is present.

(2) If the keys are not placed in a sealed container, an inventory of keys will be made by serial number or by other identifying information on the key (for example, a stamped number on the key). The inventory and change of custody will be recorded on DA Form 5513-R.

l. Combinations to locks on vault doors or GSA-approved security containers will be changed annually or on change of custodian, armorer, or other person having knowledge of the combination; or when the combination has been subject to possible compromise. Combinations will also be changed when a container is first put into service.

(1) The combinations to security containers will be recorded using SF 700, sealed in the envelope provided, and stored in a container meeting the storage requirements of AR 380-5 and USAREUR Supplement 1. No other written record of the combination will be kept.

(2) Controls will be established to ensure that envelopes containing combinations to locks or containers are not made available to unauthorized personnel.

m. The replacement of lock cylinders and broken keys for high-security locks may be requested through normal supply channels. Requests must be coordinated through the key custodian.

3-9. CONSOLIDATED ARMS ROOMS

a. When more than one unit uses the same arms room, each unit’s weapons should be separated by a cage or partition, when possible, and each area should be identified by unit. Weapons should always be stored in separate, locked racks or containers and marked with the unit designation.

b. The operation of a consolidated arms room requires the establishment of a landlord-tenant relationship or a bilateral-storage agreement (fig 3-6). This agreement is required to identify responsibilities for PS, set up proper SOPs, and outline accountability procedures.

c. The bilateral-storage agreement must address—

(1) The maximum number of weapons to be stored.

(2) Physical safeguards.

(3) The frequency of and the responsibility for physical inventories and reconciliation.

(4) The reporting of losses for investigation.

(5) Key-control procedures.

MEMORANDUM FOR All Unit Commanders Storing Weapons in (*Unit or Facility*) Arms Room

SUBJECT: Bilateral Storage Agreement for Consolidated Arms Room

1. As the host commander with overall responsibility for the (*unit or facility*) arms room, I am establishing this agreement. All undersigned tenant commanders and their arms-room personnel who share the use of this facility will strictly adhere to the following bilateral storage agreement.

a. Maximum quantities to be stored. Quantities of weapons to be stored will not exceed those authorized by the unit TDA or TOE, contingent on adequate space being available. Do not store ammunition in this facility except in limited quantities to support armed-guard requirements or for authorized training. Obtain written authorization from the undersigned host commander.

b. Physical safeguards. Each unit will install supply caging to separate one unit's weapons from another (where available). Spot-weld or peen all cage bolts and join the caging to prevent access to the arms room. Equip each unit's caging with its own GSA-approved locks and keys; the appropriate unit key custodian will control both. If no supply caging is used to separate one unit's weapons from another, space separation will be maintained and approved racks and containers used to secure each unit's weapons.

c. Frequency of and responsibility for inventories or reconciliation. Individual units are responsible for conducting their own inventories. (*This applies only to arms rooms where unit weapons are adequately separated and accessible only to unit personnel. In cases where all weapons are accessible to anyone entering the arms room, a physical count of all weapons must be conducted on entry and exit of the arms room. If a discrepancy is discovered during a physical count, a serial-number inventory of all the weapons will be conducted immediately. Monthly serial-numbered inventories would remain an individual unit responsibility.*) Units will provide results of monthly inventories to the commander responsible for overall security of the arms room.

d. Reporting losses for investigation. (*Develop this part locally among the commanders having weapons stored.*)

e. Key control. (*Incorporate the need for the primary key custodian controlling the IDS and vault door keys to receive current unaccompanied-access rosters from each unit in the arms room. Also emphasize the need for each unit to control and account for its own arms-room keys.*)

f. (*Unit*) has overall responsibility for this storage facility. (*Identify the unit or activity that has overall responsibility for the consolidated arms room facility.*)

g. Procedures for authorization and identification of individuals to receipt for and take physical custody of AA&E. Commanders will maintain current access rosters identifying who can sign for keys and gain unaccompanied access to the arms room by each unit. Provide copies of rosters to the unit that has overall responsibility for the arms room. Limit the number of individuals on each access roster to only those essential for mission accomplishment. In all cases, follow appropriate accountability and control procedures in AR 190-11.

h. Guard procedures for IDS failure. (*Establish procedures for guarding the arms in the event of IDS failure.*)

i. Noncompliance with procedures. Deny units not complying with these procedures access to the arms room and its weapons.

2. The POC is (*rank and name*), DSN (*telephone number*).

*Host Commander
Signature Block*

*Tenant Commander
Signature Block*

*Tenant Commander
Signature Block*

Figure 3-6. Bilateral Storage Agreement for Consolidated Arms Room

(6) Which unit will have overall responsibility for the storage facility.

(7) Procedures for the authorization and identification of individuals to receipt for physical custody of AA&E.

(8) The maximum amount of ammunition authorized for storage to support armed-guard requirements (for example, in case of IDS failure, to transport weapons), as necessary.

(9) Who will provide guards when required.

d. The agreement must be updated on change of command by the landlord or tenant unit or activity.

e. The determination of who serves as landlord should be based on staffing levels, frequency of access, and the ability to handle daily arms-room requirements. Normally, the senior commander will serve as the landlord.

3-10. ARMED-GUARD REQUIREMENTS

The term “armed guard” is defined in paragraph 3-2b.

a. If an IDS fails, an armed guard will be posted by the unit responsible for the AA&E facility until the IDS is returned to normal operation.

b. Armed guards will accompany all shipments of AA&E when transported off an installation according to AE Regulations 55-4 and 55-355.

c. Security-force personnel (for example, guards, security patrols, security-reaction forces) will be armed.

d. Unit armorers may be armed depending on the local threat and location of the storage facility.

e. When vehicles or aircraft are uploaded with ammunition, armed guards will be provided.

f. If the arming of guards off a military installation is prohibited by local law, compensatory security measures will be taken.

3-11. INTRUSION DETECTION SYSTEMS

a. General.

(1) Arms rooms storing category II arms; GSA-approved, class 5 weapons storage cabinets; and GSA-approved security modular vaults will be equipped with an approved IDS.

(2) Category II facilities without operational IDSs require continuous surveillance by armed guards.

(3) Category III and IV military weapon facilities require only continuous surveillance.

(4) All arms rooms that are not continually staffed or under continuous surveillance will be protected by an approved IDS consisting of at least two types of sensors and a duress (hold up) switch. One sensor must be volumetric (passive infrared or microwave). A balanced magnetic switch mounted on the arms-room door is considered to be the second sensor device. The IDS must comply with the requirements in AR 190-11, paragraph 3-6.

(5) The IDS must give an audible alarm at a central monitoring station or point from which a response force can be dispatched.

(6) Facilities off military installations must have a local alarm installed on the outside of the building in addition to being connected to a central monitoring station.

(7) Each arms room must have an IDS sign (fig 3-7) in English and the host-country language affixed at eye-level on the outside of each outside wall that has an entrance to the protected area.

(8) Units and activities with IDSs in remote civilian communities may arrange for alarms to be connected to a local police station, private security company, or another local monitoring service from which local civilian police can be dispatched. A commercial answering service or dial-in and playing of a recorded message is not authorized.

(9) The IDS will be tested monthly and the test must be documented. A record of these tests must be kept for at least 1 year.

(10) Personnel performing maintenance on the IDS will be escorted at all times. The date, time, type of service performed, and the names of the maintenance personnel will be documented.

(11) Electrical power-distribution panels or circuit-breaker panels will be locked at all times when not in use to prevent someone from shutting off the power to the IDS panel.

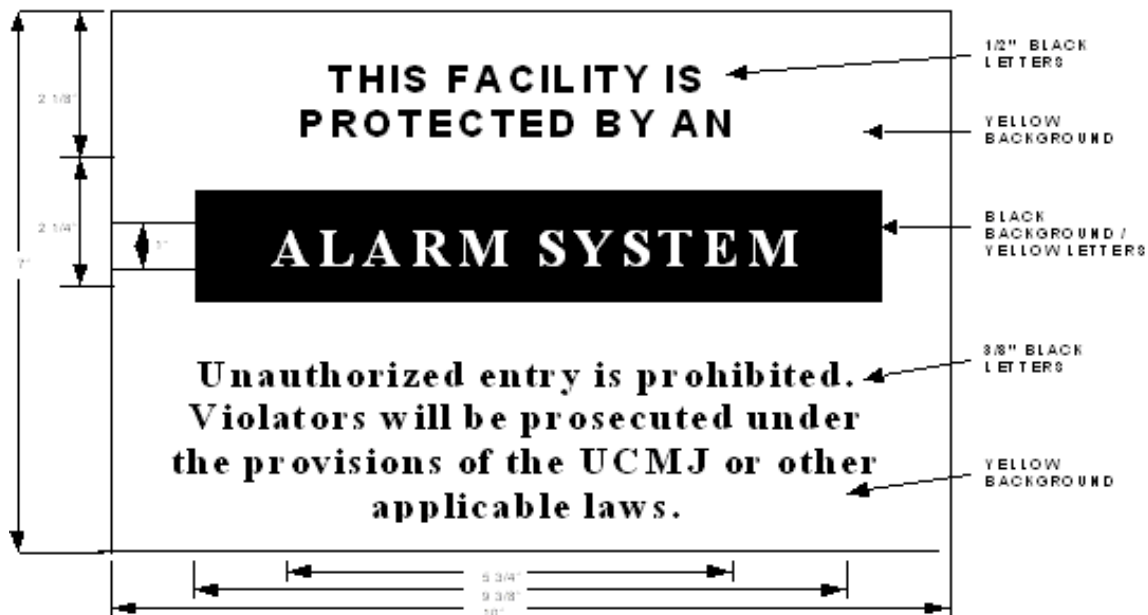


Figure 3-7. Intrusion Detection System (IDS) Sign

b. IDS Key Control.

- (1) IDS keys must be stored separately from administrative keys. These keys must be accessible only to individuals whose official duty requires them to have access.
- (2) Keys required for maintenance of the IDS must be kept separate from other AA&E and administrative keys.
- (3) The IDS key and day gate key must be placed on a separate ring from AA&E keys.

3-12. PROTECTION OF ARMS

Arms, including firearms in rod and gun club facilities, will be stored in an arms room, modular vault, or an arms-storage building according to this chapter and AR 190-11.

a. Arms and ammunition may be stored in or mounted on the tank, vehicle, or aircraft to which assigned when storage in an arms room, modular vault, or building impedes training or operational requirements. When weapons or ammunition are stored in or mounted on tanks, vehicles, or aircraft, armed guards will be provided for protection.

(1) Commanders will use appropriate security measures to ensure weapons stored in or mounted on tanks, vehicles, or aircraft are protected at all times. The following guidance applies:

(a) When not in use, tanks, vehicles, and aircraft containing weapons will be parked inside a secure motor pool or parking area. The motor pool or parking area must be under constant surveillance by armed guards and protected according to level III security measures as prescribed by AR 190-51, paragraphs 3-3 and 3-5. These motor pools and parking areas will be segregated from other areas on the installation by a perimeter fence or other approved barriers.

(b) When operational readiness permits, weapons that are accessible and easily removable will be dismounted and secured inside the locked tank, vehicle, or aircraft, or at another approved location.

(c) Weapon systems that are impractical to dismount because of operational readiness or the possibility of damaging the weapon system will be made inoperable by removing an essential component or components. Electrical power may be considered an essential component (for example, on 20- and 30mm weapon systems).

(d) Ammunition for weapons systems will not be stored on board tanks, vehicles, or aircraft if electrical power is the only essential component removed from the weapon system. In this storage configuration, level II security measures must be followed according to AR 190-51, paragraphs 3-3 and 3-5.

(2) Large weapons (for example, crew-served weapons and mortar tubes) that cannot be secured in arms rooms or other arms-storage facilities because of inadequate storage space may be—

(a) Stored in locked, completely enclosed armored vehicles. In these cases, the security requirements in (1) above apply.

(b) Secured at other secure locations, such as a room made secure by compensatory measures. In these cases, protection and surveillance by guards or other personnel will be provided according to the risk category of the weapons involved. These weapons will be rendered inoperable according to (1)(b) above.

(3) During maintenance-support operations, weapon components will be stored in a storage facility that meets security requirements according to the risk category of the items involved.

(4) STCs and BSB commanders may authorize the storage of small quantities of category IV arms in GSA-approved, class 5 security containers that do not contain and are not used to store classified documents or material without having an IDS or meeting security-lighting and security-patrol requirements. The commander will decide on the quantity to be stored based on mission and operational requirements in conjunction with an assessment of the vulnerability, safety, and threat conditions. These provisions apply only to small units (for example, USACIDC detachments) that must store a small quantity of prescribed weapons for operational requirements.

b. Individuals issued or in possession of arms are responsible for the security of the arms while they are entrusted to their care.

(1) Each weapon issued for training, operations, or other reasons will be carried at all times on the person of the individual to whom it was issued or will be properly safeguarded and secured. Except during emergencies, weapons will not be entrusted to the custody of any other person except those responsible for the security of operational weapons. These persons will comply with issue and turn-in procedures. Local procedures will be established to secure and account for the weapons of personnel who are medically evacuated during training.

(2) During field exercises and training, pistols and revolvers issued to personnel will be secured in an authorized, military-issue holster and secured to the person by a military-issue lanyard (national stock number (NSN) 8465-00-965-1705).

(3) Pistols and revolvers that lack a device to affix the lanyard will be secured by running the lanyard through the weapon trigger guard during field and training exercises. If the weapon must be drawn and used for a current operation, the commander may waive this requirement.

(4) The USACIDC may authorize individuals to keep their assigned weapons in their private quarters as dictated by operational requirements. In these instances, the USACIDC will establish accountability safeguards and security measures.

3-13. STORAGE AND SUPPLEMENTAL CONTROLS

a. New facilities built for storage of category II arms will meet the facility criteria in AR 190-11, appendix G.

b. An existing facility in which categories II, III, and IV arms are stored together will meet the criteria for facilities storing category II arms in AR 190-11, appendix G, unless the facility has equivalent or better security.

c. Category II arms stored in arms-storage buildings or rooms that do not meet or exceed the security criteria for category II arms must be stored in one of the following:

(1) A GSA-approved, class 5 security container that does not contain and is not used to store classified documents or material.

(2) A safe-type, steel file container that does not contain and is not used to store classified documents or material. The container must have a three-position, dial-type, combination lock that provides protection against forced entry as approved by the GSA (Federal Specification AA-F-363B, as amended).

(3) An approved modular vault that does not contain and is not used to store classified documents or material, with GSA-approved, class 5 vault doors or GSA-approved, class 5 armory doors. Modular vaults meeting Federal Specification AA-V-2737 may be used to meet this requirement.

d. Category II arms stored in vaults, containers, and safes must be under 24-hour armed-guard surveillance or protected by an approved IDS, and the facility must be checked by a security patrol at least once every 8 hours.

e. Categories III and IV arms should be stored in facilities meeting or exceeding the criteria in AR 190-11, appendix G.

(1) Categories III and IV arms stored in facilities that do not meet or exceed the criteria for categories III and IV arms must be stored in a GSA-approved, class 5 security container that does not contain and is not used to store classified documents or material; or a safe-type, steel file cabinet, that does not contain and is not used to store classified documents or material, and that provides forced-entry protection as approved by the GSA (Federal Specification AA-F-363B, as amended).

(2) Containers weighing less than 500 pounds must be fastened to the structure.

f. Category IV arms that are stored in unmanned facilities not equipped with an IDS will be checked by a security or guard patrol at irregular intervals of not more than 24 hours.

3-14. ARMS RACKS AND STORAGE CONTAINERS

a. When not in use, arms will be stored in banded crates, metal containers, approved standard-issue racks, or locally fabricated arms racks, and secured in approved weapons-storage facilities. Approved standard-issue metal wall lockers or metal cabinets may be used. Crates or containers will be banded, locked, or sealed in a way that prevents weapons from being removed without leaving visible signs of tampering. Screws or bolts used in assembling containers, lockers, and cabinets will be made secure to prevent disassembly.

b. All arms racks and containers will be locked with approved secondary padlocks.

(1) In facilities that are not manned 24 hours a day, rifle racks and containers weighing less than 500 pounds will be fastened to the structure, or fastened together in groups so that the total weight is more than 500 pounds, using bolts or chains equipped with secondary padlocks.

(2) Bolts used to secure racks will be brazed, peened, or spot-welded to prevent easy removal. Chains used to secure racks and containers will be of heavy-duty, hardened, galvanized steel with welded straight links at least 5/16-inch thick; or will provide the equivalent resistance against the force required to cut or break a secondary padlock. Hinged locking bars for racks must have the hinge pins welded or otherwise secured to prevent easy removal.

c. Locally fabricated racks and modified metal wall lockers will provide, as a minimum, the security equivalent of standard-issue racks or containers. All racks and containers will be constructed to prevent the removal of a weapon by disassembly.

(1) Servicing logistics assistance representatives (LARs) and battalion command-level representatives will jointly perform certification and authorize the use of the locally fabricated racks or containers. Once certified by the LAR, the racks and containers will be considered DA-approved and must be stamped with a serial number.

(2) The using unit will maintain the certification on file in the location where the racks are used. The BSB PS office may be contacted for information on servicing LARs.

d. When weapons are in transit, stored in depots or warehouses, or held for contingencies, the weapons crates or containers do not need to be fastened to the structure. However, these crates or containers must be banded or locked and sealed in a way that will prevent weapons from being removed without leaving visible signs of tampering. The facilities and buildings in which these weapons are stored will meet the structure and other security requirements of this regulation. Arms being unpacked or packed for shipping or that are in assembly-line configuration in a maintenance repair or rebuild facility do not require storage in racks or containers. However, the facilities in which they are stored will meet the structure and other security requirements of this regulation.

3-15. SECURITY LIGHTING

a. Interior and exterior lighting will be provided for all arms-storage buildings, buildings in which arms rooms are located, and arms rooms. The lighting will be adequate enough to allow guards (or individuals responsible for maintaining surveillance) to see the unauthorized removal of arms and other illegal acts, such as forced entry, during hours of reduced visibility.

b. Areas appropriate for lighting include entrances to buildings, corridors, and arms rooms. When an arms room is located inside a building, the entrance door to the arms room will be illuminated. Arms rooms that are located inside another room (for example, a supply room) do not require security lighting over the arms-room door. However, when an arms room is located inside another secured room, the exterior door to that room will be illuminated.

c. Security lighting will also be provided for motor pools, hangars, and outdoor parking areas for vehicles or aircraft that have weapons installed or stored on board.

d. Switches for exterior lights will be installed so that they are not accessible to unauthorized individuals.

e. Exterior lights will be covered with wire mesh or equipped with vandal-resistant globes that will prevent the lights from being broken by thrown objects.

3-16. DOORS, LOCKS, AND LOCKING DEVICES

a. Except for GSA-approved, class 5, steel vault doors with built-in, three-position, changeable combination locks, doors used for access to arms rooms or structures will be locked with an approved, high-security locking device or high-security padlock and hasp providing comparable protection to the locks.

(1) An approved, high-security shrouded hasp will be used to secure categories I and II AA&E storage facilities to enhance their security. Doors used for access to arms rooms will be locked with approved locks and hasps.

(2) In existing storage facilities equipped with double-door protection, high-security padlocks and hasps will be used on the most-secure door. Secondary padlocks will be used to secure the second door providing protection under the double-door concept. Other openings that cannot be secured from the inside with locking bars or deadbolts (for example, issue windows and portals) will be secured on the inside with approved secondary padlocks.

(3) When high-security hasps are installed, locking bars and T-pins should be left in place to help with opening and closing the doors and to prevent misalignment of the hasps.

(4) "Panic hardware," when required, will be installed to prevent the door from being opened by tampering from the outside. Panic hardware will meet safety, fire, and building codes and must be approved for and in compliance with host-country requirements as applicable.

b. Facilities in which vehicles or aircraft are stored with sensitive items on board will be secured by approved secondary padlocks. Aircraft will be secured with manufacturer-installed or -approved modification work order door-locking devices when not in use. All hatches and other openings to tracked vehicles that cannot be secured from the inside will be secured from the outside with approved secondary padlocks.

3-17. CONTROL OF WEAPONS

a. Weapon Control. Weapons will be controlled as follows:

(1) Armorers and custodians will keep a master authorization list (MAL) (fig 3-8). The MAL will have the names and unit or organization of the persons who will receive issues, and the number of equipment receipts. The MAL must be kept updated to show personnel changes. Before a weapon is issued, the armorer or custodian must compare each person's DA Form 3749 with the MAL to prevent unauthorized issue of weapons.

(2) Armorers and custodians will prepare DA Form 3749 for each privately owned or individually assigned weapon and give the receipt to the person who owns or is assigned the weapon. A new DA Form 3749 will not be prepared when the responsible officer or manager changes. Copies of DA Form 3749 issued by previous responsible officers or managers will be accepted as long as the bearer of the card is validly listed on the MAL. A new DA Form 3749 must be prepared if an old one is lost, mutilated, or destroyed, or when a new member joins or is assigned to a unit or activity.

(3) The use of DA Form 3749 for the issue and turn-in of rod-and-gun-club-owned weapons that are loaned or rented is required. Club armorers or custodians and patrons will sign each weapon out on a weapons control log and sign it back in before the rod and gun club closes. Patrons are prohibited from taking or transporting club-owned weapons off club grounds.

(4) When individually owned or assigned weapons are issued, the receiving person must turn in his or her DA Form 3749 for the weapon to the person making the issue. The recipient and armorer will make an entry on AE Form 190-13I (app E) or a locally reproduced form that includes the same information. The recipient will enter in ink the nomenclature and serial number of the item received, the time of issue, and his or her signature as it appears on the DA Form 3749. Component items such as gloves, spare barrels, and tripods must be included on the hand-receipt.

(5) When weapons are turned in, the control sheet must be closed out and the person's DA Form 3749 must be returned. The armorer or custodian receiving the weapon will enter the date, time, and his or her initials on the control sheet.

(6) The weapons control log will be kept in the unit or activity active file until completion of the next monthly inventory by serial number. Control logs will be kept for at least 6 months.

(7) When a single weapon is needed for issue to more than one person, DA Form 3749 must be prepared for each person authorized to use the weapon. The weapon must be issued according to (1) through (4) above, except that control-log entries are required, regardless of the time for which the weapon is issued.

(8) When other than individually assigned weapons are issued, hand-receipt or temporary hand-receipt procedures will be used. Control-log entries are also required.

b. AE Form 190-13I.

(1) AE Form 190-13I will be used to issue weapons (including privately owned weapons). If, however, a military weapon is issued for less than 24 hours, AE Form 190-13I is not required unless ammunition is issued with the weapon.

(Unit Name)

Master Authorization List (MAL): Custodians of arms will maintain a current MAL that identifies the individual owner of each weapon or the individual to which each weapon is assigned.

Container/ Rack No.	Weapon Type:	Weapon Serial No.	Assigned To:	Owner/ Rank	Equipment Receipt No.	Remarks
1	M16A2	1004589	Smith, John J.	E5	12	
2	M16A2	1347802	Jones, James A	E4	27	In for maintenance
3	M16A2	1019876	George, Ken B.	E2	36	
4	M-9	45A23987	Williams, Ken R.	O3	68	

NOTE: List all weapons in custody.

Figure 3-8. Master Authorization List (MAL)

(2) Before issuing a weapon using AE Form 190-13I, the armorer must receive DA Form 3749 for the weapon from the individual. When the individual returns the weapon, the armorer will return the DA Form 3749.

(3) AE Form 190-13I will be kept until the monthly inventory is completed. The form may be destroyed after the inventory unless the inventory reveals a discrepancy (for example, if a weapon is still signed out), in which case the form will be kept until the discrepancy is resolved.

(4) DA Form 2062 may be used instead of DA Form 3749.

3-18. PROTECTION OF MISSILES, ROCKETS, AMMUNITION, AND EXPLOSIVES AT UNIT LEVEL

a. Unit-level stocks are those stored in basic-load quantities (quantities stored in tactical configuration for readiness and emergency purposes) or that are on hand for operational and training purposes. AR 385-64 and USAREUR Regulation 385-64 must be used to determine the maximum permissible storage amounts and the appropriate configuration of ammunition and explosives.

b. A typical facility for storage of operational quantities of ammunition would be a building used to store ammunition on a rifle range or an MP or guard (security) arms room. These facilities will comply with the requirements for unit arms rooms.

c. The following are minimum requirements for safeguarding and maintaining unit-level stocks:

(1) Depending on tactical and contingency considerations, unit-level stocks will be stored in approved ammunition-storage rooms or magazines.

(a) Commanders may authorize in writing the storage of small quantities of ammunition in unit arms rooms after an ammunition-safety survey has been completed and an ammunition-storage license has been granted by the ASG or BSB safety office. The authorization will be posted in the arms room.

1. The amount of ammunition stored must be consistent with operational requirements.

2. Ammunition authorized for storage in unit arms rooms will be stored in approved containers.

Ammunition will be secured in banded crates, approved metal containers, or approved standard issue, commercial, or locally fabricated cabinets. Approved, standard-issue, metal wall lockers may be used. Security containers (GSA-approved, class 5) that do not contain and are not used to store classified documents or material may also be used.

3. Crates will be banded or sealed in a way that prevents ammunition from being removed without leaving visible signs of tampering. Ammunition stored in metal containers and cabinets will be secured with secondary padlocks. Screws and bolts used in assembling containers, lockers, and cabinets will be made secure to prevent disassembly. Containers weighing less than 500 pounds will be fastened to the structure, or fastened together in groups so that the total weight is more than 500 pounds, using bolts or chains equipped with secondary padlocks.

(b) Commanders will establish security procedures for issuing basic-load ammunition that will enable the unit to accomplish its combat or contingency missions. When tactical, operational, or readiness conditions permit, basic-load ammunition will be stored in ammunition-storage rooms or magazines that have equivalent structural standards as those prescribed for the risk category of the items being stored.

(c) For safety and accountability reasons, live ammunition will not be stored in weapon magazines in the arms room.

(2) When operational and training requirements prevent the storage of unit-level stocks or explosives in ammunition-storage magazines, these stocks may be stored in or on combat vehicles, aircraft, ships, or trailers, or in other configurations as required by the operational environment. When stored in this manner, each storage area will be under continuous surveillance by an armed guard.

(3) Ammunition and explosives may be stored on board vehicles and aircraft if the vehicle or aircraft is located inside a motor pool or park or aircraft parking area. When stored this way, the area will be under continuous surveillance by armed guards.

(4) Vehicles and aircraft with missiles and rockets in a ready-to-fire configuration will be under continuous surveillance by armed guards.

(5) Ammunition and explosives in open storage (such as aircraft cargo areas, ammunition supply points (ASPs), and vehicle-holding areas) will be under continuous surveillance by armed guards. Ammunition and explosives in temporary open storage will be secured using the following:

(a) A perimeter barrier, either temporary or permanent.

(b) Armed-guard surveillance (installation guards or on-duty personnel). Guard personnel must use an effective communication system.

(c) Security lighting during hours of darkness or reduced visibility.

(d) Inventory, accountability, and control procedures.

(e) Restricted-area signs.

(f) Controlled access.

(6) When more than one unit uses the same area, stocks will be separated and identified by unit. One unit will be designated as responsible for the security of the entire area, including access control.

(7) When the threat or other conditions dictate, commanders will decide whether or not to store missile battery coolant units (BCUs) separately from the weapon.

d. The following are additional minimum requirements for safeguarding and maintaining category I missiles at deployment ammunition holding areas (AHAs) and at unit areas:

(1) Unit-level stocks of category I missiles will be stored in ammunition-storage rooms, modular vaults, or magazines.

(2) Vehicles and aircraft storing category I missiles will be under 24-hour surveillance by armed guards who maintain continuous, unobstructed observation of the vehicle or aircraft. When stored this way, the supplemental security measures in AR 190-51, paragraphs 3-3e(3) and 3-5e(8), also apply.

(3) Category I missiles will not be stored in open storage (for example, aircraft cargo holding areas, vehicle holding areas, AHAs, ASPs). Category I missiles at these locations will be secured as follows:

(a) Items must be placed in approved containers (container express (CONEX), military-owned demountable container (MILVAN), or military container moved via ocean (SEAVAN)) or in a completely enclosed storage structure. The doors will be secured with two approved medium- or low-security locks.

(b) The category I storage area must have 24-hour armed-guard surveillance.

(c) The two-person rule must be followed for access.

3-19. WEAPONS AND AMMUNITION INVENTORIES

a. The following inventory procedures will be used when the responsibility for custody of arms-storage-facility keys is transferred between authorized persons:

(1) Both the incoming and outgoing custodians will conduct a physical inventory of the weapons and ammunition. (In consolidated arms-storage facilities where access to weapons and ammunition is restricted because of the physical layout, both persons will verify that each person who had access to weapons and ammunition has made a physical count.) If a specific quantity of materiel is being stored in the arms room in locally banded and sealed containers, these items will be recorded on DA Form 2062 as "Container protected by seal # that contains X rounds of Y ammunition." A separate entry will be made for each container in the item-description block of DA Form 2062 with the quantity listed as 1. DA Pamphlet 710-2-1, figure 9-3, is an example of this posting.

(2) The results of the inventory will be recorded on DA Form 2062. Completed forms will be kept until the next serial-number inventory (b below) is completed. At that time, the forms may be destroyed. If differences are found during the serial-number inventory and are not resolved, the forms must be kept as an exhibit for a report of survey.

(3) The person receiving the keys to the arms-storage facility will receipt for the weapons and ammunition. This person must enter his or her signature, rank, and current date on the inventory form in the column where the inventory quantity is listed. DA Pamphlet 710-2-1, figure 9-3, is a sample DA Form 2062 used for recording weapons and ammunition inventory results.

b. A monthly inventory of weapons by serial number will be conducted by the responsible officer (1LT or above) or a disinterested NCO (SFC or above), warrant officer, commissioned officer, or DOD civilian (GS-09 or above) appointed by the responsible officer. The same person will not conduct this inventory in consecutive months. The unit armorer will not conduct this inventory but may help with the inventory process. The following procedures will be used for the inventory:

(1) Compare the serial number of the weapons with those listed on the property book, hand-receipt, or sub-hand-receipt, as appropriate. Make a list of any differences. Prepare and process an after-action report (AAR) to correct differences within makes or models.

NOTE: Serial-number differences will not be corrected using an AAR. Accountability for serial-number differences will be established according to AR 735-5.

(2) If weapons or ammunition have been signed out or turned in for maintenance, proper supporting documentation must be maintained and verified. The inventorying officer must record this on inventory sheet after verification.

(3) Inventory ammunition by listing it by purpose (for example, basic load, operational load, training), Department of Defense identification code (DODIC), lot number, quantity on hand, and quantity signed out on the inventory form. List quantities shown on banded or sealed and banded containers. Do not break manufacturer, ASP, or quality assurance specialist (ammunition surveillance) (QASAS) seals for the inventory. Record any tampering, damage, or broken seals or bands and notify the commander immediately.

(4) Record the results of the inventory in a memorandum. The use of a computer printout or a preprinted memorandum listing serial numbers is authorized. Indicate in the memorandum any weapons signed out or in maintenance. Record the quantity of loose ammunition and banded or sealed containers in the memorandum. Seal numbers for individual containers should be listed. The person conducting the inventory will sign the inventory memorandum. According to AR 190-11, chapter 6, keep the inventory memorandum for 2 years if no discrepancies were noted, or 4 years if a discrepancy was noted. Figure 3-9 is a sample record of a serial-number inventory.

MEMORANDUM FOR RECORD

SUBJECT: Monthly Serial-Numbered Inventory of Arms and Ammunition

1. A monthly inventory was conducted of all assigned weapons, ammunition, and sensitive/high value items. No discrepancies were noted during the inventory.
2. The following items were accounted for:
 - a. Weapons.

Type:	Model:	Serial Number:
Rifle	M16A1/M203	7469339
Rifle	M16A1/M203	7469340
Rifle	M16A1/M203	7469341
Rifle	M16A1/M203	8765744
Rifle	M16A1/M203	9874653
Machinegun	M60	5856555
Machinegun	MK19	6768881
Pistol	45 Cal.	M8487

- b. Ammunition.

Type:	Amount:	Lot Number:
7.62mm	40 rounds	Y17A
5.56mm	150 rounds	Y21B
9mm	200 rounds	B12B
45 Caliber	15 rounds	H54B

3. All the ammunition was accounted for. One 9mm pistol, serial number M988341, could not be located and is unaccounted for. The pistol has been reported as missing and an investigation is being conducted.

*Signature Block of Individual
Performing the Inventory*

*Signature Block of Individual
Performing the Inventory*

Figure 3-9. Monthly Serial Number Inventory Record

(5) Immediately report any discrepancies to the responsible officer. If any question on serviceability arises (for example, damaged containers, seals tampered with or broken), contact QASAS personnel for serviceability verification. The ASP for the unit or activity should be able to provide the information needed to contact QASAS personnel.

(6) The responsible officer will report discrepancies to the property book officer. The property book officer will conduct causative research for these discrepancies. Causative research includes but is not limited to comparing all postings to the applicable property book page against documents that support those postings, verifying hand-receipt-change documents, searching storage areas controlled by the property book officer, and ensuring that the end-item identity was not destroyed by consolidation, disassembly, or mislabeling. If no conclusive findings are made, the following actions will be taken:

(a) Turn in overages as “found on installation” property.

(b) Account for shortages according to AR 735-5, chapter 13.

(c) Post adjustment documents to the property book and adjust hand-receipts or sub-hand-receipts accordingly.

3-20. REPORTING MISSING OR RECOVERED AA&E

When AA&E is lost, missing, stolen, or recovered, provost marshals or designated representatives will complete DA Form 3056 within 72 hours and send one copy to each of the following addresses:

a. OPM, HQ USAREUR/7A (AEAPM-SO), Unit 29931, Bin 153, APO AE 09086-9931.

b. 202d Military Police Group (CIRCE-ZA), Unit 29201, APO AE 09102-9201.

c. HQDA (DAMO-ODL-S), 400 Army Pentagon, Washington, DC 20310-0400.

3-21. SECURITY OF AA&E DURING TRAINING AND ON SHIPS

Specific criteria and standards for protecting AA&E during training and on ships, including in shipboard armories, will be developed by the major subordinate or tenant command concerned based on this regulation. AA&E deployed in the field for training or operational purposes will be secured at all times. The deploying commander will establish and enforce procedures for securing deployed AA&E based on an assessment of the threat, objectives, location, and the duration of the deployment. The following guidelines apply:

a. AA&E will be under continuous physical control (properly handled and secured at all times).

b. AA&E will not be left unattended or unsecured.

c. Persons charged with the custody of AA&E will be able to sound an alarm if a forceful theft is attempted.

d. A response force will be available to protect the AA&E.

e. A system of supervisory checks will be established to ensure all personnel comply with security procedures.

Supervisory checks of the AA&E holding area will be made to ensure the AA&E being guarded has not been tampered with.

f. The control of ammunition and explosives during field training or range-firing will be monitored closely by all officers, NCOs, and civilian equivalents. On completion of training, the area will be policed and unused ammunition and explosives collected for turn-in. Personnel will be checked closely to ensure unused ammunition and explosives are not retained. Close supervision by officers, NCOs, and civilian equivalents can eliminate most security problems in the training area.

g. The selection of personnel to perform guard duties at AA&E holding areas will be closely monitored by commanders to ensure only responsible individuals are assigned duty.

3-22. COMMERCIAL WEAPONS AND AMMUNITION

a. Commercial arms and ammunition in stock or maintained by non-appropriated fund activities and installation-approved private organization activities will be protected according to security and accountability procedures equal to those prescribed in this chapter for military arms and ammunition.

b. Commands will stop the sale or possession of weapons and ammunition by non-appropriated fund activities that fail to comply with this chapter.

(1) During non-duty hours, commercial arms and ammunition will be stored in facilities meeting the requirements of this paragraph. The storage area will be protected by a certified and approved IDS.

(2) When displayed, arms and ammunition will be under the surveillance of sales personnel. Arms and ammunition will be secured to prevent loss or theft as follows:

(a) Ammunition equal to 1 day's estimated sales may be displayed in a locked showcase or security case or fixture. If possible, empty boxes will be displayed in showcases and sales will be made from reserve stock.

(b) Gun and ammunition fixtures will be locked except when merchandise is presented to the customer for inspection.

c. Resale arms and ammunition, club-owned arms, and privately owned weapons and ammunition will be separated from each other and secured in separate, locked containers.

d. For safety and accountability, live ammunition will not be stored in weapon magazines in the arms room.

3-23. PRIVATELY OWNED WEAPONS AND AMMUNITION

a. Commanders will ensure that privately owned weapons and ammunition (including authorized war trophies) are protected on their installations and facilities. Commander's will—

(1) Ensure all privately owned weapons have been registered with the USAREUR central registry (AE Reg 190-6).

(2) Secure privately owned arms and ammunition in an approved arms room and in approved locked containers separated from other AA&E. For safety and accountability, live ammunition will not be stored in weapon magazines in the arms room.

(3) Account for and inventory privately owned arms and ammunition each month in the same manner as military arms and ammunition.

(a) Ensure DA Form 3749 is issued for each privately owned weapon secured in the arms rooms.

(b) Establish limits in writing on the quantity and type of privately owned ammunition stored in the arms room, based on space availability and safety considerations.

(4) Post applicable policy and host-nation information on ownership, registration, and possession of weapons and ammunition on unit and activity bulletin boards.

(5) Conduct inspections according to AR 190-11 and this regulation to ensure proper storage and control.

(6) Process unauthorized AA&E according to AR 190-22, paragraph 3-4.

(7) Prohibit the retention and storage of incendiary devices and explosives in unit and activity arms rooms.

(8) Brief all newly assigned persons on this regulation and on subordinate command guidance. All personnel will be informed of changes.

b. When stored in an arms room, privately owned weapons must be able to be inventoried by serial number. The only authorized way to conduct this inventory is as follows:

(1) Weapons may be left in an unlocked, private weapons case so that the case can be opened and serial numbers verified.

(2) Weapons may be inventoried and secured inside a container with a lock and serial-numbered seal in a way that would prevent the weapons from being removed without leaving signs of tampering.

(a) A copy of the inventory must be placed inside the container before sealing it.

(b) The serial number on the seal must match the inventory document that identifies by serial number what is inside the case or container.

c. Personnel who have weapons (including authorized war trophies) and ammunition in their possession or who store them at rod and gun clubs or in unit arms rooms will—

(1) Comply with Army and Army in Europe regulations (for example, AE Reg 190-6) and host-nation laws on ownership, possession, registration, off-post transport, and use.

(2) Follow local security and safety regulations. Also safeguard the unit- or activity-issued DA Form 3749 for turn-in to the unit or activity armorer when the weapon is withdrawn from the arms room.

(3) Withdraw privately owned weapons and ammunition from the unit arms rooms only on approval of the unit commander. The unit commander may grant approval only if the individual or owner—

(a) Has a *Waffenbesitzkarte* (German Weapons Permit).

(b) Is shipping the weapon back to the United States.

(c) Intends to sell, transfer, or dispose of the weapon.

(4) Notify the local provost marshal office if a loss occurs.

3-24. SECURITY PATROLS AND CHECKS

a. A security or guard patrol or unit personnel will periodically check containers, facilities, and areas used to store AA&E. Checks will be conducted on an irregular basis during non-duty hours to avoid establishing a pattern. Security checks will be made to ensure unauthorized personnel are not in the area and that structures are intact and have not been broken into. Supervisory checks will be conducted to ensure guard duties are being performed properly.

(1) For categories I and II facilities protected by an IDS, the intervals between checks will not exceed 8 hours.

(2) For categories III and IV facilities, the intervals between checks will not exceed 24 hours, or 48 hours if the facility is protected by an IDS.

b. Facilities storing arms outside a military installation will be equipped with an IDS and checked by a security patrol on an irregular basis at least once every 24 hours.

c. Security patrols may be conducted by military or civilian security personnel, including contract guards.

d. Security-force personnel must be provided with an adequate means of communication.

e. Guard procedures will be reviewed at least annually and revised if necessary to provide greater application of security measures, and will place special emphasis on guard post locations and guard orientation on duties to be performed.

f. Inspections and guard checks will be increased at nighttime and on weekends and holidays to deter violations and allow for losses to be detected quickly. These checks will be recorded and will consist of an inspection of the building or facility, including all doors and windows. Records of these checks will be maintained in an active file for at least 90 days and then destroyed.

g. Law-enforcement patrol plans will be coordinated and integrated with the guard plan or other security plans and programs to the maximum extent possible. When facilities are located in civilian communities, liaison will be established with local civilian-police agencies to ensure that periodic surveillance is conducted and that a coordination plan for security exits.

h. Personnel conducting security checks or performing guard duties are forbidden from climbing onto any objects, vehicles, railcars, or containers to check locks, seals, or other items. This policy applies to checks conducted at home station and while in-transit.

i. Security and guard personnel are forbidden from conducting security “penetration tests” that involve climbing on fences or other objects to test security methods or response procedures.

3-25. TRAINING

Commanders and managers responsible for AA&E will establish a training program for personnel responsible for the security and accountability of these items. Annual refresher training will also be conducted to ensure that all personnel are aware of their responsibilities for controlling and safeguarding AA&E.

3-26. IN-TRANSIT SECURITY OF AA&E

The minimum-security requirements for the in-transit movement of AA&E are outlined in AE Regulation 55-4, section IV; and AE Regulation 55-355, chapter 8.

CHAPTER 4 ACCESS CONTROL

4-1. PURPOSE

This chapter—

a. Prescribes policy, procedures, standards, and guidance for the design, construction, and operation of installation access-control points (ACPs) in the European theater. The construction guidance provided is applicable to both new construction and ACP renovations.

b. Prescribes general policy for controlling entry into and exit from military installations.

c. Will be used with Technical Manual 5-853-2, AE Regulation 190-16, and USAREUR Regulation 525-13.

NOTE: USAREUR Regulation 525-13 prescribes policy and procedures for physically searching individuals and vehicles.

4-2. ACCESS METHODS

a. 100-percent positive identification of all personnel is required for access to all U.S. Forces installations in the European Theater.

b. Personnel may be authorized access to U.S. Forces installations by any of the following means:

(1) The person has a valid DOD identification card and is registered in the IACS.

(2) The person has a valid installation pass or a temporary installation pass. A valid installation pass with temporary duty (TDY) orders will authorize access when an individual must temporarily exceed his or her access level for operational reasons. For example, if an installation-pass holder has a 6th ASG-wide installation pass but must attend training in the 26th ASG AOR, his or her installation pass and TDY orders that state the training location and timeframe may be used to obtain access.

(3) The person is signed in and escorted by an individual with sign-in privileges.

(4) The person is on an approved access roster and presents one of the following documents:

(a) Passport.

(b) Personal identification card issued by the country of citizenship (for example, German *Personalausweis*, Belgian identity card, Italian *carta d'identità*).

(c) Military identification card issued by one of the Sending States (Belgium, Canada, France, the Netherlands, and the United Kingdom).

c. AE Regulation 190-16 provides detailed information on policy and procedures for gaining access to U.S. Forces installations.

4-3. ACCESS-CONTROL POINTS

Installation commanders will allocate resources necessary to enforce access controls and establish a method for verifying compliance with policy and procedures.

4-4. ACP PROCEDURES

a. Installation commanders will execute access-control procedures according to AE Regulation 190-16 and this chapter.

b. Commanders will ensure that all guards (contract and borrowed military manpower (BMM)) perform cursory visual inspections of the interior of vehicles as they conduct identification checks on vehicle occupants. When something or someone appears suspicious, the vehicle will be diverted for a more thorough search.

c. Communication between ACP guards and search teams must be established to alert the search teams of suspicious vehicles.

d. Guards will conduct threat-focused searches of vehicles and large containers. Emphasis will be placed on searching vehicles such as commercial vans and trucks, delivery and cargo-type vehicles, and vehicles that do not have U.S. Forces license plates. Emphasis will also be placed on searching containers and the personal baggage of work crews who must be signed onto the installation.

e. During periods of greater threat, such as during holidays, special events, or anniversaries, commanders must increase the frequency and locations of searches of vehicles entering their installations.

f. Commanders will ensure that all guards (contract and BMM) receive proper and continuous training on effective vehicle-search techniques. Search personnel must be proficient in detecting not only the obvious, but also in noticing modifications that may indicate the presence of hidden compartments or explosives. Commanders should refer to the DOD Technical Support Working Group (TSWG) Vehicle Inspection Checklist as a guide for developing and conducting training on search techniques.

g. Guards should also be trained to note operator and passenger behavior through means such as casual questions while checking identification to help verify their purpose for entering the installation.

h. Commanders will continuously check to ensure guards thoroughly understand the commander's intent and comply with policy on access control, arming, rules of engagement (ROE), and use of force.

i. ACP guards will use AE Form 190-13H(G) (English/German) or AE Form 190-13H(I) (English/Italian) as applicable at every ACP to manually log in visitors and their vehicles. ACP guards will record visitor information electronically once the ACP is equipped with an IACS computer terminal.

4-5. ACCESS CONTROLS FOR DELIVERIES AND CONTRACTOR BUSES

a. Delivery personnel and contract bus drivers must be listed on a current, approved access roster or have a valid DOD identification card or installation pass to be granted unescorted access to a U.S. installation. If delivery personnel have a valid DOD identification card or installation pass, or are listed on a current access roster, they may be granted unescorted access.

b. Personnel who do not have a valid DOD identification card or installation pass and who are not listed on an access roster must be signed in at the gate and escorted at all times by a valid identification-card holder or installation pass holder with sign-in privileges.

c. Sponsoring activities receiving regular deliveries must request and obtain installation passes for all regular delivery personnel according to AE Regulation 190-16.

(1) If an installation pass is not authorized, sponsoring activities must provide a current access roster through the servicing BSB. Sponsoring activities will not give access rosters to ACPs. Access rosters must be consolidated and verified by the BSB and distributed to the respective ACPs.

(2) If installation passes or access rosters are not used, the sponsoring activity or individual must sign in delivery personnel and escort them continuously until they depart the installation.

d. If delivery personnel, contract bus drivers, or individuals require access and have not been issued a valid pass, are not on a valid access roster, and do not have an escort present, access-control personnel will contact the BSB provost marshal office (MP desk) for assistance and resolution. The BSB provost marshal office will attempt to contact the appropriate agency or recipient of the delivery. The responsible agency or recipient must go to the ACP and either sign in the delivery or bus personnel if required and provide continuous escort or decline the access request.

e. Activities using large-scale contract delivery services (for example, the USAREUR personal property shipment program and the United States Army Transportation Management Center, Europe) will—

(1) Develop and distribute a Microsoft Excel spreadsheet that includes all information required for an installation access roster according to AE Regulation 190-16. The roster will be forwarded to each BSB installation-access control office with a request for distribution.

(2) Take the steps necessary according to AE Regulation 190-16 to obtain an installation pass for all full-time and select personal-property shipment pick-up and delivery contracted-service personnel.

f. ACP guards will check pick-up and delivery documents to ensure that the location is correct before allowing access.

g. If discrepancies regarding the driver, vehicle, or shipment are identified (for example, serial-numbered seals have been tampered with, removed, or broken), the subject vehicle will be searched, the driver will be detained, and the incident will be reported to the MP.

h. Only DOD identification-card holders or valid installation-pass holders with sign-in privileges may sign in and escort personnel.

4-6. ACP GUIDANCE

a. Considerable emphasis must be placed on the design of an ACP. Commanders should use measures (for example, bollards, road spikes) to prevent vehicles from entering an installation through exit lanes in conjunction with the use of serpentine barriers.

b. Each ACP has different types of construction and traffic flow. For this reason, specific operational guidance must be in the commander's SOP and special guard instructions. Paragraph 4-8 provides basic recommendations for manning and operating ACPs.

c. Before an ACP is constructed or renovated, a traffic survey must be conducted. The survey must analyze traffic patterns that support or will be affected by the construction or renovation of the ACP. The survey also helps with the proper placement and layout of each ACP.

(1) An ACP should be located inside the installation at a distance that will allow vehicles to line up without creating an off-post traffic problem. Gates should be positioned before the security checkpoint to allow access to the visitor office.

(2) Inbound traffic should be physically separated from the outbound traffic lane, and both lanes should be able to be closed or blocked completely. Consideration must be given to advances in technology that can increase installation security. Pedestrian and bicycle access must be available.

(3) The installation must coordinate with local host-nation officials regarding traffic flow. Two types of barriers must be considered: those designed to channel traffic and those designed to stop it.

d. "ACP" is an inclusive term for eleven functional components that must be integrated to accomplish the access-control mission. Commanders should consider these components when constructing or upgrading an ACP. Paragraph 4-7 describes these components and provides recommended minimum requirements that will guide in ACP construction and upgrade.

e. Functional layouts and designs of typical ACPs are covered by the Technical Manual 5-853 series and Military Handbook 1013/14, provide conceptual functional layouts for ACPs. Figures 4-1 and 4-2 are examples of conceptual functional layouts. ACP signs and signposts are shown in figures 4-3 and 4-4. Actual ACPs must be adapted to meet specific site-layout requirements and restrictions. Appendix B provides barrier guidelines.

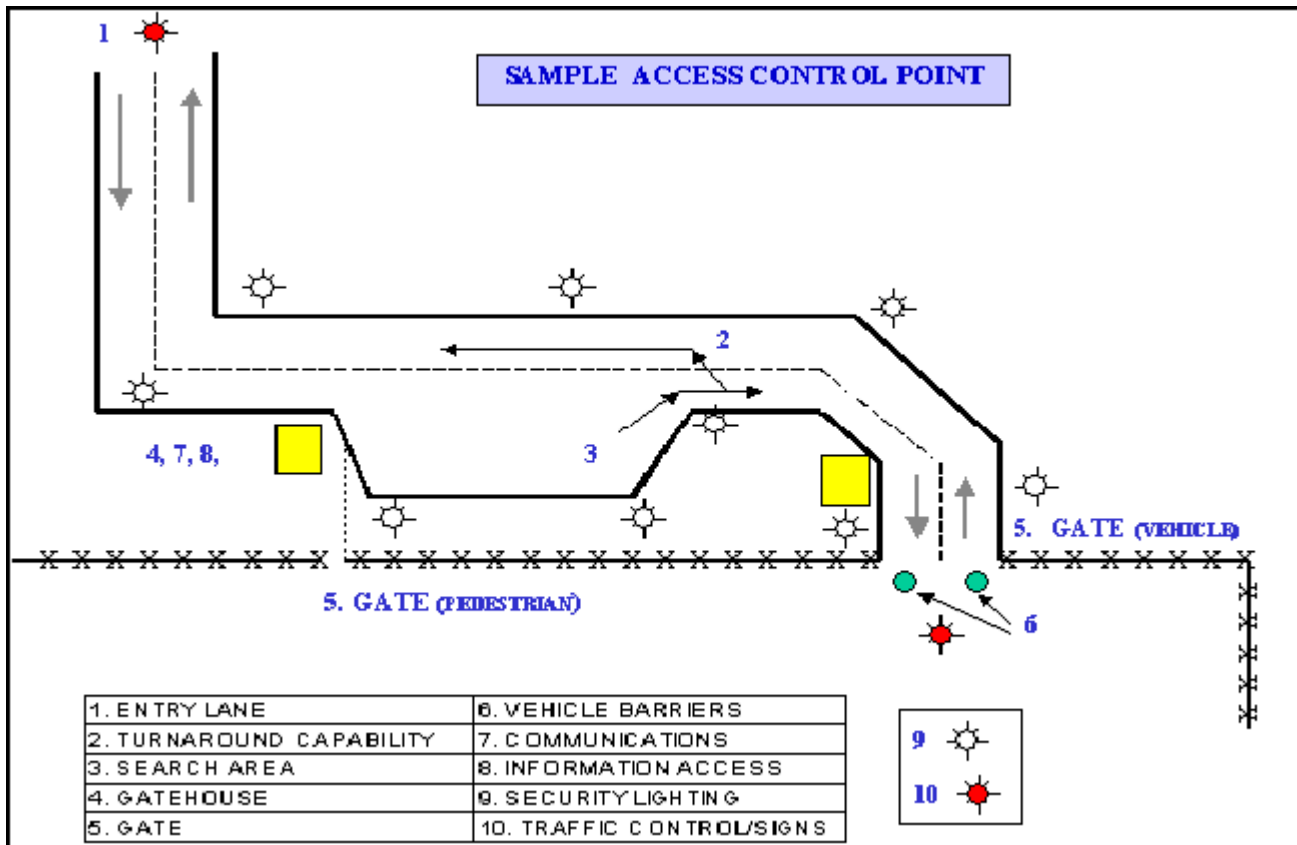


Figure 4-1. ACP Conceptual Functional Layout 1

f. The Engineering Division, IMA-Europe, sponsors the Security Engineering Design Course. This course is taught by the USACE Protective Design Center. The target audience for this course includes BSB DPW employees, antiterrorism officers, and PS specialists. This course offers training on the fundamentals of security engineering design with a concentration on ACP design. The key instructional manuals used in the course are the Technical Manual 5-853 series.

g. The OPM is the proponent for ACP operational guidance. The Office of the Deputy Chief of Staff, Engineer, HQ USAREUR/7A, is the proponent for engineering and design guidance.

4-7. ACP DESIGN STANDARDS

a. ACP Categories. ACPs generally fall into one of two categories:

(1) Permanent ACP. A permanent ACP is one that has a permanent gate located with a secure, fenced perimeter. It consists of all eleven components listed in subparagraph b below.

(2) Temporary ACP. A temporary ACP is one that has an entry lane but no gate or fence. It consists of components 1, 2, 5, 7, 10, and 11 in subparagraph b below. Component 4 (search area) is required where possible.

b. Functional Components. Depending on the category, ACPs will include some or all of the eleven components listed below:

(1) Entry Lanes. Permanent or temporary barriers must be used to separate traffic lanes at ACPs to prevent unauthorized lane changing. The minimum number of lanes depends on the rate of traffic flow.

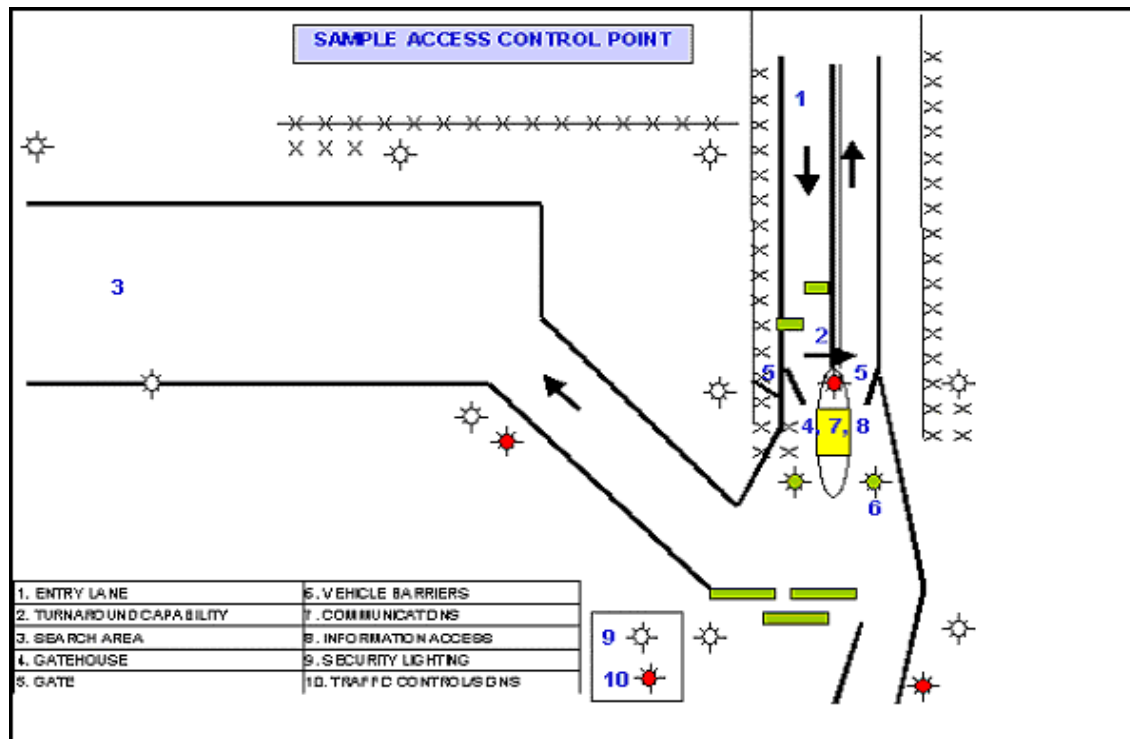


Figure 4-2. ACP Conceptual Functional Layout 2

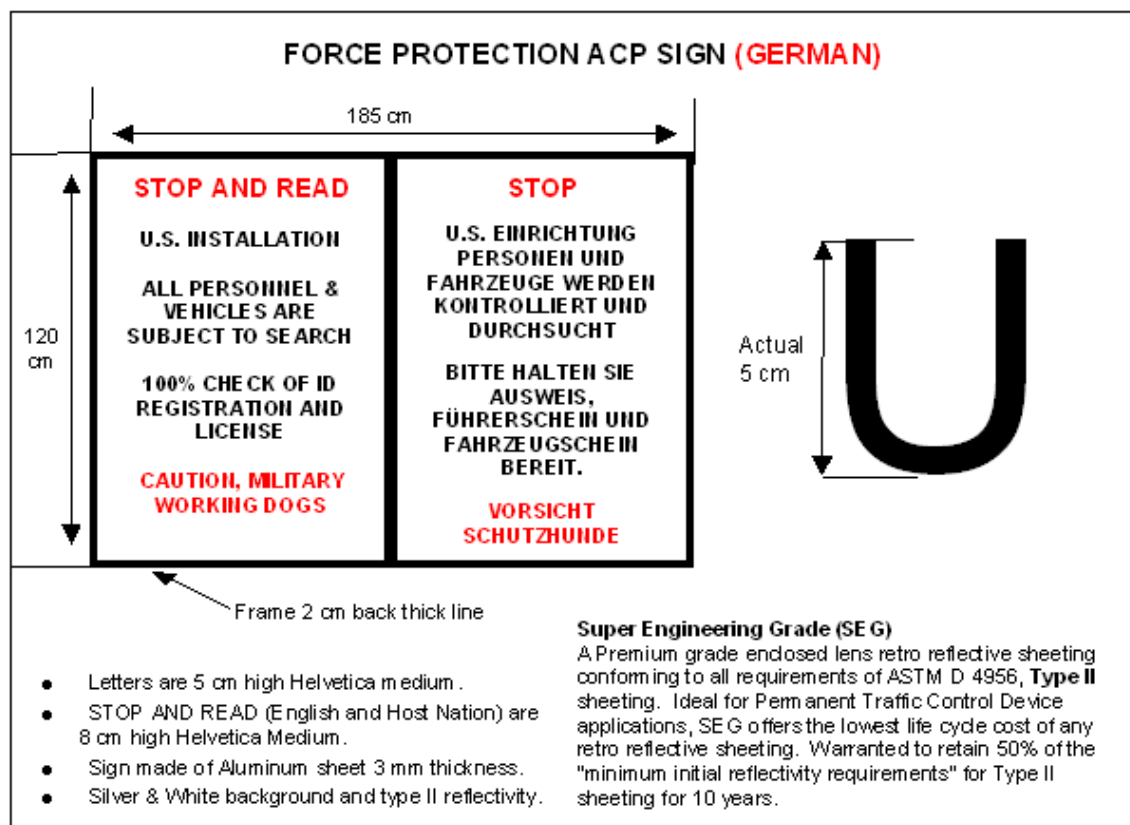


Figure 4-3. Force Protection ACP Sign

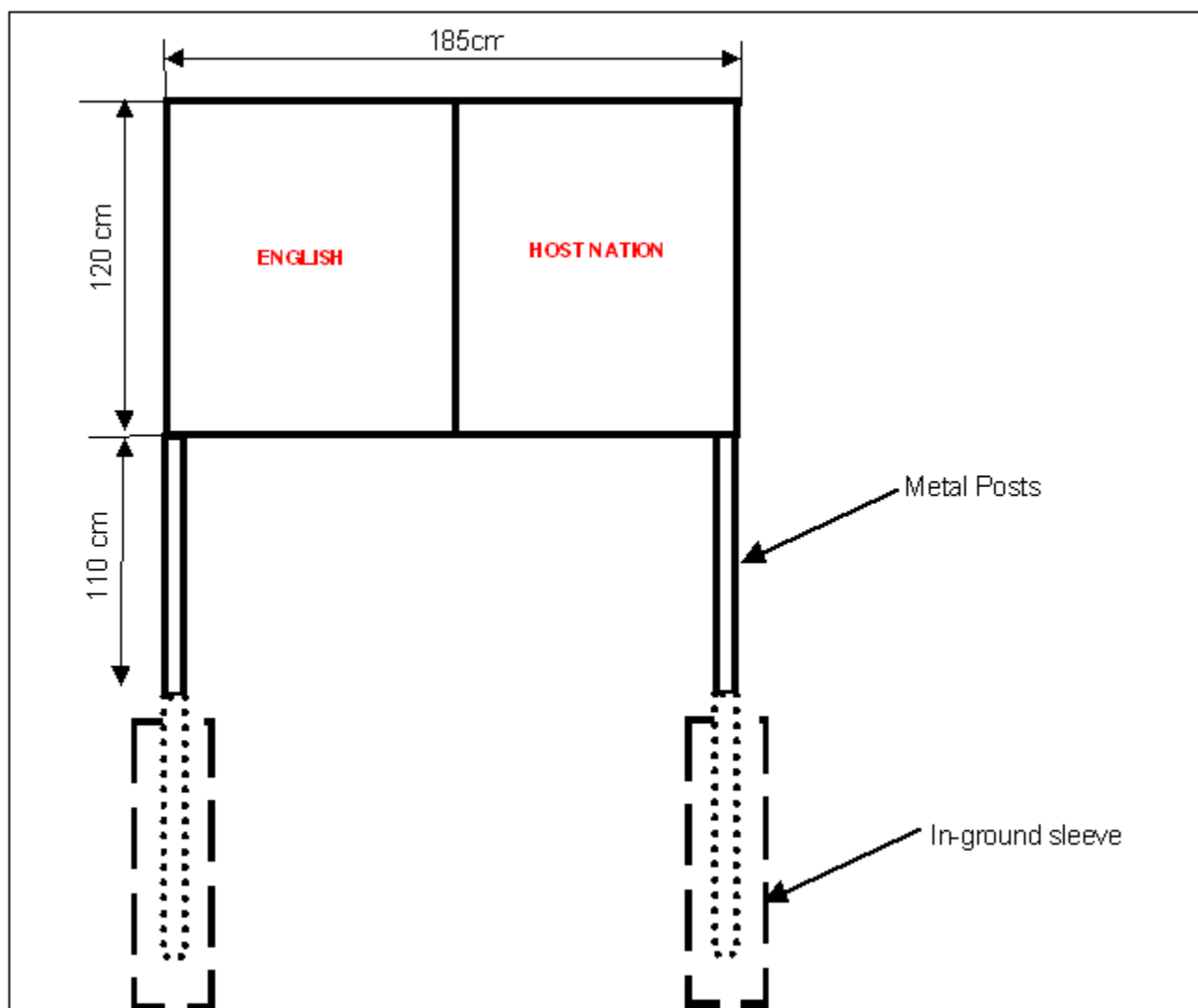


Figure 4-4. Force Protection ACP Signposts

(a) ACPs should have a separate lane or lanes where traffic requires additional access-verification checks (for example, individuals being signed in or who are listed on access rosters).

(b) Slow-moving traffic should be able to pull over to avoid impeding traffic flow.

(c) Pedestrian traffic and the visitor sign-in area should be separated from the vehicle lanes and should have a dedicated parking area to avoid crossing traffic. Having both vehicular and pedestrian traffic at the identification checkpoint distracts guards and increases liability and safety concerns. The resulting confusion increases the chance that unauthorized vehicles or pedestrians can gain access. Therefore, the visitor sign-in area should be located before the identification checkpoint. Pedestrians should be guided to the checkpoint and kept separate from vehicle traffic for safety and control purposes.

(2) Exit Lanes. Exit lanes should have a means of slowing and stopping a vehicle that tries to enter the installation using an exit lane. Barrier placement is critical. Creating serpentines, short-angle turns, and tighter turn radii help slow vehicles down. Barriers and other devices (such as vehicle-tire spikes) should be considered as means to stop a vehicle.

(3) Turn-Around Capability. The ACP should be designed so that vehicles of any size that are not granted access to the installation are able to turn around before entering. The turn-around should be accomplished within the area controlled by ACP operational personnel.

(4) Search Area. ACPs should designate areas that are adequate for vehicle searches. The area should be safely segregated from the main traffic flow and should be large enough to hold a tractor-trailer. Search areas should be located outside the installation where possible. If not possible, search areas should be located inside the installation and maintained at an adequate distance from inhabited structures as prescribed by the most-stringent applicable AT/FP standards (currently 45 meters). Search areas should be covered when possible to help to protect guard personnel and ACP equipment from extreme temperatures and adverse weather conditions.

(5) Gatehouse/Guard shack. The gatehouse or guard shack, the guards and their equipment, together serve as the center of ACP operations. At some locations, additional structures may be used to provide protection for personnel conducting security operations.

(a) The gatehouse or guard shack should—

1. Be at least 7.5 square meters, but may vary in size. The structure should have enough counter space for writing reports, storing reference books, and holding a computer workstation and other needed items. Interior storage space should be enough for storing cleaning materials and special equipment.
2. Have at least a 1-meter overhang above the doors to protect the guards against the weather.
3. Meet the ballistic protection level of H.P. White Level 1 (capable of withstanding three rounds of 9mm, full-metal copper jacket ammunition with a velocity of 358 meters/second).
4. Be heated and include a latrine facility with a sink and interior storage room. An exterior storage facility for traffic cones, portable barricades, and signs should be provided as needed.
5. Be placed on a raised curb area and will have nonskid floors.

(b) Prefabricated portable facilities or tents may be used for small or temporary ACPs as determined by the installation commander.

(c) Enough parking space should be provided in the vicinity of the gatehouse to facilitate security-vehicle stationing and shift changes of gate personnel.

(d) Electrical power equipment should be protected by an uninterrupted power supply and include the following:

1. Heavy-duty, exterior power outlets sufficient for outdoor heaters and temporary floodlights.
2. Interior power outlets sufficient for radio chargers, computers, and hand-held searchlights.

(6) Gates. Gates are not required if the ACP remains open at all times. Appendix B provides barrier requirements and guidance on contingencies for closing the roadway. If the ACP is not open 24 hours a day, 7 days a week, a gate is required that is capable of completely stopping the flow of traffic and restricting vehicles according to the same USAREUR minimum vehicle standard as specified for barriers. Vehicle-penetration distance for gates should be determined based on the location of the nearest inhabited structure to the gate area while considering the standoff distance according to the most-stringent applicable AT/FP standards. Gate and fence or barriers should prevent unauthorized entry. The locking device for the gate should be tamperproof and not accessible from the outside.

(7) Barriers and Crash Cushions. Barriers are devices that physically restrict the movement of vehicles and pedestrians. Crash cushions are structures that protect gate personnel from being injured by vehicles.

(a) ACPs without gates should have enough barriers on site or available if contingencies call for the complete closure of the roadway.

(b) Barriers and crash cushions, such as concrete jersey barriers, planters, and stationary concrete or metal bollards, should be used to protect ACP gatehouses. Moveable or retractable barriers should be used and located in such a way that entry and exit lanes can be secured to prevent entry onto the installation.

(c) Barrier requirements will be determined by a local threat or vulnerability assessment but must not be less than the minimum vehicle standard of 15,000 pounds at 30 miles per hour, which is equivalent to the kinetic energy of 450,000 pound-feet (610KN).

(d) For part-time ACP operations, barriers should be available for positioning to prevent vehicles from circumventing the designated ACP. Reducing the speed of vehicles approaching the ACP to a level below those that permanent, active barriers could stop is critical. This can be accomplished through the use of serpentine barriers that create tighter turns.

(8) Communications. ACPs should have two means of communications with a central monitoring point (normally the supporting MP station). One means should be a direct-ring telephone line to the MP desk, while the second may be a radio, cell phone, or both.

(9) Information Access. ACPs should have access to a computer capable of displaying information such as “be on the lookout” (BOLO) alerts, installation-bar list, and vehicle-registration data. The fielding of the IACS will automate many procedures now being done manually (for example, sign-in and access-roster procedures and scanning the installation-bar list).

(10) Security Lighting. Lighting at all ACPs should be appropriate to act as a deterrent and to allow guards to perform their security functions. All ACPs should be provided with lighting adequate for navigation through gates and for conducting required nighttime searches and other security functions. Standards should be according to Technical Manual 5-811-1, chapter 11. Additional portable light sets may also be used.

(11) Traffic-Control Devices and Signs. Traffic-control devices and signs include signs, road markings, and traffic signals. These devices should be adequate to direct traffic, provide security-information requirements, and provide appropriate safeguards to both guards and drivers. All traffic-control devices and signs should comply with local host-nation standards and be in English and the local language.

4-8. ACP MANNING RECOMMENDATIONS

The following positions are recommended for conducting permanent ACPs. Manpower availability, ACP layout, the FPCON, and other considerations will influence the manning level.

a. One point man. One guard will be posted at the ready position at the main entrance into the gate (the first person seen as vehicles enter). For safety reasons, this guard must not be positioned too close to a major thoroughfare. The “ready position” means that the M4 or M16 will be carried so that the barrel is pointed downward at a 30- to 40-degree angle. The weapon will be oriented across the soldier’s body. All soldiers will maintain awareness of the muzzle orientation of their weapon. All pistols will remain holstered.

b. Two or three identification-checkers and traffic-controllers. Another guard (the next person seen by arriving vehicles) working with the contract guards will direct the flow of vehicles through the gate or to the inspection area. A contract guard may substitute for the second guard for short periods. Contract guards are intended to be access-document-verification experts.

c. Three-person vehicle-inspection team (two searchers and one inspection-team supervisor).

(1) Vehicle-inspection teams must stay concentrated on their mission during duty. Teams will use the DOD TWSG Vehicle Inspection Checklist during inspections and should report to duty fully trained on inspection procedures. Information on obtaining this checklist is available at http://www.tswg.gov/tswg/prods_pubs/vicpress.htm. Teams will inspect the vehicle and execute the checklist with precision. Weapons should not be carried if they will interfere with searches, but should be readily accessible and properly secured at the search point.

(2) The inspection-team supervisor will be at the ready position and from a reasonable distance will direct the driver and passengers out of the car, issue the driver clear instructions, and maintain his or her ready position. This person is responsible for armed over watch of the search process. Over-watch personnel will be armed according to current FP guidance.

d. One sergeant of the guard (SOG) or commander of the relief. This is the senior-ranking individual assigned over-watch, supervisory, or leadership duties. This individual will coordinate ACP duties with the contract guards and direct the use of contract guards, as necessary, within the scope of the guard contract.

CHAPTER 5

SECURITY OF ARMY PROPERTY AT UNIT AND INSTALLATION LEVEL

5-1. GENERAL

a. This chapter highlights key areas and supplements the minimum-security standards required for safeguarding unclassified and non-sensitive Army supplies and equipment at the unit level as described in AR 190-51. AR 380-5 and USAREUR Supplement 1 provide information on the security of classified information and equipment.

b. The first step in determining the minimum level of security required is the completion of a risk analysis. The unit commander or designated representative and the PSO or PSI will conduct a joint risk analysis. DA Pamphlet 190-51 provides the background and an explanation of step-by-step procedures for determining minimum-security requirements and conducting a risk analysis for categories of Army property. Completing a risk analysis is fairly complex and requires assistance from PS personnel.

c. A risk analysis will be conducted on all MEVAs—

- (1) When a unit or activity is activated.
- (2) When a unit permanently relocates to a new site or facility.
- (3) When no formal record exists of a previous risk analysis.
- (4) At least every 3 years or more frequently at the discretion of the unit or activity commander.
- (5) During the planning stages of new facilities, additions to facilities, and facility renovations.
- (6) When an incident occurs in which an asset is compromised.

d. Risk level I security standards for both physical-protection and security-procedural measures are considered to be the least restrictive, and risk level III security standards are the most restrictive. All units and activities must meet at least the security standards for risk level I.

e. Identifying all the minimum PS standards that must be in place for the different types of Army property is beyond the scope of this regulation. The following is a list of the different references where security requirements are covered in detail:

- (1) Aircraft and components at Army aviation facilities (AR 190-51, para 3-3).
- (2) Aircraft and components not at Army aviation facilities (AR 190-51, para 3-4).
- (3) Vehicles and carriage-mounted or towed weapons systems and components (AR 190-51, para 3-5).
- (4) Communications, electronics equipment, and night-vision devices (AR 190-51, para 3-6).
- (5) Organizational clothing and individual equipment (OCIE) stored at central issue facilities (AR 190-51, para 3-7).
- (6) OCIE not stored at central issue facilities (AR 190-51, para 3-8).
- (7) Subsistence items stored at commissaries, commissary warehouses, and troop issue subsistence activities (TISAs) (AR 190-51, para 3-9).
- (8) Subsistence items not at commissaries, commissary warehouses, or TISAs (AR 190-51, para 3-10).
- (9) Repair parts at installation-level supply support activities and direct support units with an authorized stockage list (ASL) (AR 190-51, para 3-11).
- (10) Repair parts not at installation-level support activities and direct support units (AR 190-51, para 3-12).
- (11) Petroleum, oils, and lubricants (POL) at bulk storage facilities (AR 190-51, para 3-13).

- (12) POL not at bulk storage facilities (AR 190-51, para 3-14).
- (13) Facility engineering-supply and construction-material storage areas (AR 190-51, para 3-15).
- (14) Audiovisual equipment, training devices, and subcaliber devices at training and audiovisual support centers (TASCs) (AR 190-51, para 3-16).
- (15) Audiovisual equipment, training devices, and subcaliber devices at units or activities that are not at TASCs (AR 190-51, para 3-17).
- (16) Aircraft and vehicles with classified onboard equipment or components (AR 190-51, para 3-18).
- (17) General civilian and military personnel (AR 190-51, para 3-20).
- (18) Industrial and utility equipment (AR 190-51, para 3-21).
- (19) Hand tools, toolsets and -kits, and shop equipment (AR 190-51, para 3-22).
- (20) Administrative and housekeeping supplies and equipment (AR 190-51, para 3-23).
- (21) Unit supply rooms (AR 190-51, para 3-25).
- (22) Postal facilities and operations (USAREUR Reg 600-8-3).
- (23) Medical facilities, supplies, and equipment (AR 190-51, chap 4).
- (24) Museums (AR 190-51, chap 5).
- (25) Banks and credit unions (DOD Inst 1000.12 and Department of Defense Financial Management Reg, vol 5, chap 34).
- (26) Army and Air Force Exchange Service (AAFES) facilities (AR 60-10).
- (27) AAFES Exchange Operating Procedures 16-1.
- (28) Military working dog (MWD) kennel facilities (DA Pam 190-12, chap 7).
- (29) Defense Commissary Agency facilities (DOD Dir 5105.55)

5-2. COMMUNICATIONS SECURITY (COMSEC) MATERIAL AND CONTROLLED CRYPTOGRAPHIC ITEMS

AE Regulation 380-40 provides policy and procedures for safeguarding, controlling, and disposing of COMSEC material, controlled cryptographic items (CCIs), and other secure communications equipment.

5-3. SECURITY OF NIGHT-VISION DEVICES

- a. The loss of NVDs is unacceptable. Not only is the financial loss significant, but the use of stolen NVDs by terrorists or other criminal elements makes the security of NVDs a serious issue.
 - b. Commanders at all levels must assign a high priority to the security and accountability of NVDs.
 - c. As a minimum, NVDs will be stored in a secure storage structure meeting the requirements in AR 190-51, appendix B.
 - d. NVDs will be segregated from other items using approved metal wall lockers, security cabinets, or caging.
- (1) Cages inside secure storage structures storing NVDs must—

- (a) Be constructed of material that is equal to or greater than 6-gauge, cold-drawn, steel wire mesh with a grid of not more than 2 inches center to center.

- (b) Have all bolts welded or peened.
- (c) Be anchored to the floor.
- (d) Either extend to the ceiling or have a top.

(2) Metal wall lockers or security cabinets used inside a secure storage area to secure NVDs will meet all the same construction standards of those used to store arms inside an arms room.

e. Storage on open shelving is not acceptable unless the shelves are inside a steel cage and that is inside a secure storage structure.

f. The doors to steel cages, metal wall lockers, and security cabinets storing NVDs will be secured using an Army standard (American Series 5200) padlock.

g. Keys to NVD cabinets, lockers, and cages must be secured and controlled at all times and will be maintained and issued separately from other keys.

h. GSA-approved class 5 or 6 security containers that do not contain and are not used to store classified documents or material may be used to store NVDs.

i. Commanders may authorize the storage of NVDs inside locked armored vehicles or aircraft if the armored vehicles or aircraft are parked inside a fenced motor pool with adequate security lighting.

j. When removed from storage for use during training or operations NVDs will be signed out to individuals.

k. NVDs will not under any circumstances be transported in privately owned vehicles or be left unattended while not secured.

l. During shipment, commanders will ensure NVDs are not mixed with non-sensitive equipment, are secured using double-barrier protected, and are locked in containers with equipment of comparable value or sensitivity.

m. Inventories of NVDs will be conducted—

- (1) Each month by physical count while in storage.
- (2) Each quarter by serial number while in storage.
- (3) Before shipment by serial number.
- (4) On receipt of shipment by serial number.

n. While conducting inventories, each container or vehicle (if applicable) will be opened to ensure there is actually an NVD inside.

5-4. SECURITY OF GLOBAL POSITIONING SYSTEMS AND PRECISION LIGHTWEIGHT RECEIVERS

The same security requirements for NVDs apply to global positioning systems and precision lightweight receivers.

5-5. SECURITY OF U.S. ARMY-ISSUED BAYONETS

a. When not in use, U.S. Army-issued bayonets must be stored in a locked and sealed footlocker or container inside the unit arms room or another secure storage structure as prescribed by AR 190-51, appendix B. A copy of the bayonet inventory must be placed inside the container before sealing it and the original must be kept in inventory records and be available for inspection and inventory purposes. A memorandum will be placed on the outside of the container stating the contents and must include the date, seal number used to seal the container, and the two signatures of the individuals who conducted the inventory.

b. Bayonets will be inventoried each month in conjunction with the inventory of weapons. During inventories, the container storing the bayonets is not required to be opened as long as the seal is intact and there are no signs of tampering. If signs of tampering are present, the container must be opened and a 100-percent inventory must be conducted to ensure no bayonets are missing.

5-6. STORAGE STRUCTURE SECURITY

Equipment and supplies listed in AR 190-51 and this regulation must be stored in structures meeting specific security standards. AR 190-51, appendix B, provides minimum specifications for supply and equipment-storage structures.

5-7. KEYS, LOCKS, LOCKING DEVICES (INCLUDING HASPS AND CHAINS), AND PROTECTIVE SEALS

a. This section provides guidance on procedures for keys, locks, locking devices (including hasps and chains), and protective seals. AR 190-11 provides additional requirements for AA&E.

b. Only approved locks and locking devices (including hasps and chains) will be used. All questions on the identity of approved, commercial-equivalent locks and locking devices (including hasps and chains) meeting military specifications will be addressed to the Naval Civil Engineering Laboratory (NCEL). Personnel can obtain the most current version of these specifications from the NCEL (Code L56), Port Hueneme, CA 93043-4328.

c. Under no circumstances will keys, locks, or alternate keys and locks be placed in a security container that contains or is used to store classified documents or material.

5-8. KEY CUSTODIAN AND ALTERNATE CUSTODIAN

A primary or alternate key custodian will—

a. Be appointed in writing (fig 5-1) to issue and receive keys and maintain accountability for office, unit, or activity keys.

b. Ensure that individuals designated to issue, receive, and account for keys in his or her absence clearly understand local key-control procedures.

c. Maintain DA Form 5513-R at all times to ensure continuous accountability for keys of locks used to secure Government property.

d. Be listed on an access roster.

5-9. KEY CONTROL REGISTER

Keys will be signed out to authorized personnel as needed on a key control register (DA Form 5513-R). This register is approved for use to meet the requirements of this regulation. When not in use, the DA Form 5513-R will be kept in a locked container that does not contain and is not used to store classified documents or material and to which access is controlled.

5-10. KEY DEPOSITORY

a. A lockable container, such as a safe or filing cabinet, or a key depository made of at least 26-gauge steel, equipped with a tumbler-type locking device, and permanently affixed to a wall, will be used to secure keys.

b. The key depository will be located in a room where it is kept under 24-hour surveillance or in a room that is locked when unoccupied.

5-11. LOCKS

a. The use of master-key system or multiple-key systems is prohibited except as noted elsewhere in this regulation.

b. U.S. Government key-operated, pin-locking deadbolts that project at least 1 inch into the doorframe or tumbler-type padlocks will be used to safeguard unclassified, non-sensitive Army supplies and equipment if a lock is required. Selection will be based on the value of items protected, how essential the items are to the mission, and the vulnerability to attack. Questions regarding approved locks and locking devices may be addressed to the NCEL as indicated in paragraph 5-7b.

c. Padlocks that are not in use and their keys will be secured in a locked container that does not contain and is not used to store classified documents or material. Access to the container will be controlled at all times by the key custodian or person issued the keys and locks.

d. Medeco lock cylinders are the only approved locking mechanism for securing IDS control panels/boxes.

MEMORANDUM FOR RECORD

SUBJECT: Duty Appointment for (*Primary or Alternate*) Administrative Key Custodian

1. EFFECTIVE: (*date, rank or grade, name, SSN*) is appointed as the (*Primary or Alternate*) Administrative Key Custodian for the (*unit or activity*).
2. AUTHORITY: AR 190-51, appendix D.
3. PURPOSE: Assure proper control, accountability, and handling of keys and locks for the arms room.
4. PERIOD: Until officially relieved or released from this appointment.
5. SPECIAL INSTRUCTIONS: Become familiar with the key control provisions of AR 190-51.
6. POC: (*rank and name*), DSN (*telephone number*).

Unit/Activity Commander
Signature Block

DISTRIBUTION:

1-Unit/Activity Commander
1-Individual Concerned
1-Unit Physical Security Officer/NCO
1-Physical Security Files

Figure 5-1. Appointment Memorandum for Primary or Alternate Administrative Key Custodian

5-12. KEY-AND-LOCK ACCOUNTABILITY

a. Keys and combinations to locks will be accounted for at all times. Keys to locks used to protect the property of an office, unit, or activity will be checked at the end of each duty day. Differences between keys on hand and the key-control register (DA Form 5513-R) must be reconciled.

b. Padlocks and their keys will be inventoried by serial number twice a year. A written record of the inventory will be kept on file for 1 year.

c. When a key to a padlock is lost or missing, an inquiry will be conducted and the padlock replaced or re-cored immediately.

d. A key-and-lock inventory will be maintained that includes a list of all of the following:

- (1) Keys.
- (2) Locks.
- (3) Key serial numbers.
- (4) Lock serial numbers.
- (5) Location of locks.
- (6) The number of keys maintained for each lock.

e. The inventory will be secured in the key depository.

f. Padlocks and keys that do not have a serial number will be given one. This number will be inscribed on the lock or key as appropriate.

5-13. ADDITIONAL KEY-AND-LOCK CONTROLS FOR IDS AND KEY CONTAINERS

a. Keys to IDSs (operational or maintenance) and key containers will not be removed from the installation except to provide for protected storage elsewhere. Keys to locks securing key containers will be provided physical protection equivalent to that provided by the key container itself. Keys to containers and IDSs will be maintained separately from other keys and will be accessible only to individuals whose official duties require access to them.

- (1) A current roster of these individuals will be kept in the unit, agency, or organization.
- (2) The roster will be protected from view.

(3) The roster will be signed by the designated official and will include the names of individuals authorized to receive keys from the key custodian (d below).

- (4) At no time will keys be in the custody of a person not listed on the roster.

b. Keys to containers and IDSs may be secured together in the same key container. However, under no circumstances will keys and locks or alternate keys and locks be placed in a security container that contains or is used to store classified documents or material.

(1) When arms and ammunition are stored in the same areas, keys to the storage areas may be maintained together but separate from other keys that do not pertain to AA&E storage. The number of keys will be kept to the minimum required. Keys may not be left unattended or unsecured at any time.

(2) Keys required for maintenance and repair of IDSs, including keys to the control the unit door and monitor cabinet, will be kept separate from other IDS keys. Access will be permitted only to authorized maintenance personnel.

(3) IDS operational keys will be stored in containers of at least 20-gauge steel equipped with GSA-approved, low-security padlocks or GSA-approved, built-in, three-position changeable combination locks; or in GSA-approved, class 5 or class 6 containers that do not contain and are not used to store classified documents or material. Combinations will be recorded on SF 700, sealed in the envelope provided, and stored in a container according to AR 380-5 and USAREUR Supplement 1.

(4) Containers weighing less than 500 pounds will be fastened securely to the framework or masonry of the structure using approved bolts or chains equipped with approved secondary padlocks to prevent easy removal.

c. If the keys are lost, misplaced, or stolen keys, an investigation will be conducted immediately. The affected locks or cores to locks will be replaced immediately. Replacement or reserve locks, cores, and keys will be secured to preclude access by unauthorized individuals.

d. A key custodian will be appointed in writing. Only the commander and the key custodian (or alternate, if appointed) will issue keys to individuals on the key-access roster. Personnel listed on the roster may transfer custody in writing among themselves.

(1) The key custodian's duties will also include procurement and receipt of keys and locks and the investigation of lost or stolen keys. The key custodian will maintain a record to identify each key and lock and combinations to locks used by the activity, including replacement and reserve keys and locks. The record will show the current location and custody of each key and lock.

(2) DA Form 5513-R will be maintained at the unit level to—

(a) Ensure continuous accountability for keys.

(b) Ensure positive control of keys.

(c) Establish responsibility for the custody of stored AA&E. The completed DA Form 5513-R will be kept in unit files for at least 90 days and then disposed of by crosscut shredding.

e. When individuals are charged with the responsibility for safeguarding or otherwise having keys immediately available, they will sign for a sealed container of keys.

(1) A sealed container is a locked and sealed key container or a sealed envelope (SF 700 according to AR 380-5 and USAREUR Suppl 1) containing the key or combination to the key container.

(2) When a sealed key container is transferred from one individual to another, the unbroken seal is evidence that the keys have not been disturbed. The seal need not be broken to inventory the keys. However, evidence of tampering with a sealed container will require an inventory of the keys and other action as may be required by the commander concerned.

(3) If the keys are not placed in a sealed container, a key inventory will be made by serial number or other identifying information of the key (for example, stamped number on key). The inventory and change of custody will be recorded.

(4) Inventory records will be kept in unit files for at least 1 year and then disposed of by crosscut shredding.

f. Combinations to locks on vault doors or GSA-approved, class 5 or class 6 security containers will be changed annually, on change of custodian or other person having knowledge of the combination, or when the combination has been subject to possible compromise. Combinations will also be changed when a container is first put into service. The combination will be recorded using SF 700, sealed in the envelope provided, and stored in a container meeting the storage requirements in AR 380-5 and USAREUR Supplement 1. No other written record of the combination will be kept. Controls will be established to ensure that the envelopes containing combinations to locks are not made available to unauthorized personnel.

g. Requests for the replacement of lock cylinders and broken keys for high-security locks may be requested through normal supply channels. Requests must be coordinated through the key custodian.

(1) The OPM is the designated approval authority for any deviation in key-procurement procedures.

(2) In addition to normal key-and-lock requirements, aircraft and vehicle-storage facilities in which vehicles or aircraft are stored with sensitive items on board will be secured by approved secondary padlocks. Aircraft will be secured with manufacturer-installed or -approved modification work order door-locking devices when not in use.

(3) Hatches and other openings to tracked vehicles that cannot be secured from the inside will be secured on the outside with approved secondary padlocks.

5-14. CHAINS

When a chain is required for securing unclassified, non-sensitive equipment and supplies, specifications for approved chains may be obtained from the NCEL as indicated in paragraph 5-7b.

5-15. USE AND CONTROL OF PROTECTIVE SEALS

a. Purpose of the Seal. The seal is used to show whether the integrity of a storage facility, vehicle, rail shipment, or container has been compromised. A plain seal is not a lock, although combination items referred to as “seal locks” are available. The purpose of a seal, no matter how well constructed, is defeated if strict accountability and disciplined application are not maintained.

b. Seal Specifications. Seal-construction specifications should state that the seal must—

- (1) Be durable. Seals must be strong enough to prevent accidental breakage during normal use.
- (2) Have a complex design. Seals must be sufficiently complex to make the unauthorized manufacture of a replacement seal difficult.
- (3) Be tamperproof. Seals must readily provide visible evidence of tampering and be constructed in a way that makes simulated locking difficult once the seal has been broken.
- (4) Be individually identifiable. Seals must have embossed serial numbers and owner identification.

c. Ordering and Issuing Seals. Unit commanders will appoint a seal custodian in writing to be responsible for ordering and issuing seals. The source for the seals will be instructed to ship the seals to the attention of a seal custodian in that office. Seals not issued for actual use will always be secured in a locked, metal container with controlled access. Only seal custodians and alternates will have access. Recorded monthly inventories will be conducted to prevent the loss of seals.

d. Accounting for Seals. Seal custodians will maintain seal logbooks, preferably not in loose-leaf books.

- (1) The issue of seals to a using office, unit, or activity custodian will show the date of issue, the name of the recipient, and seal serial numbers.
- (2) The issue of a seal for actual use by a custodian will show the seal number, the date and time applied, identification of items to which applied (and location of the item if other than the main door), and the name of the person applying the seal. For outbound loaded trailers, railcars, and container shipments, the appropriate trailer, railcar, or container number and load destination will be noted.

e. Application of Seals. Seal custodians will—

- (1) Seal all doors and openings, not merely the main one.
- (2) Run seal straps through hasps only once. Seals wrapped around several times become illegible.
- (3) Listen for a “click” when inserting the point of the seal into the sheath.
- (4) To ensure positive closure, tug down on the strap and twist the point section inserted into the locking mechanism.

f. Checking Seals. Commands using seals will develop procedures for checking them. These procedures will include actions to be taken to break a seal and actions to be taken on finding a broken seal.

g. Disposition of Used Seals.

- (1) All shipping documents will include seal numbers. All seals will be verified using a seal log, shipping documents, or other appropriate documents before removal and disposal.
- (2) Seals must be defaced sufficiently on removal so that they cannot be used to simulate a good seal. These seals may be disposed of in normal trash.
- (3) If the user seal log is located on the same installation, the custodian will be advised of the destruction of the seal or the seal will be returned to the custodian. The custodian will annotate the date and time the seal is removed and the name of the individual who removed it across from the original entry in the seal log.

h. Changing Seals. The colors of seals will be changed periodically as an additional PS measure.

CHAPTER 6

PHYSICAL SECURITY EQUIPMENT (PSE)

6-1. PURPOSE

This chapter—

- a. Addresses Army and USAREUR standard PSE only. Chapter 9 addresses nonstandard PSE and FP equipment.
- b. Prescribes policy, standards, and procedures for selecting, acquiring, and using PSE.
- c. Will be used to develop requests for ESSs, which include IDSs, closed-circuit television (CCTV), and EECSs.
- d. Does not include procedures for sensitive compartmented information facilities (SCIFs). Director of Central Intelligence Directive (DCID) 6/9, AR 380-5, and USAREUR Supplement 1 to AR 380-5 provide the procedures for SCIFs.
- e. Will be used with DCID 6/9, AR 190-11, AR 190-13, AR 380-5, and USAREUR Supplement 1 to AR 380-5.

6-2. PSE OVERVIEW

PSE includes barriers, blast-mitigation devices, security communications systems, explosive-detection devices, ESSs, personal protective equipment, security fencing, gates, lighting, mass-notification and personnel-alerting systems, and other equipment used to physically protect and safeguard personnel, facilities, and critical assets from terrorist and criminal threats.

6-3. PROGRAM MANAGEMENT

Provost marshals will help commanders identify and develop PSE and ESS projects to meet requirements, establish standards, and ensure compatibility with existing systems. In coordination with the DPW, provost marshals will track and maintain data on IDSs and other ESSs in their AOR.

6-4. PRIORITIES

Priorities for PSE and ESSs are determined by the security or risk level of an installation or facility and the degree of protection required by regulation. Other determining factors are identified vulnerabilities and threats.

6-5. RISK ANALYSIS

A risk analysis will be conducted on all facilities and installations being considered for PSE and ESS enhancements or upgrades. The results of the risk analysis will be used during security planning to identify, assess, and validate PS requirements, including the need for PSE and ESSs.

6-6. FORECASTING REQUIREMENTS

a. Forecasting PSE Requirements. Commanders will properly forecast PSE requirements, develop cost estimates, and establish a maintenance plan before any acquisition.

(1) Proper forecasting will help ensure equipment and funds are available when the PSE is required. Forecasts will cover a 7-year period by fiscal year. Federal law mandates this requirement, which supports the Program Objective Management and Future Year Defense Plan.

(2) The forecast must—

(a) Identify the project, the location and unit or activity the project supports, and the fiscal year that the project is required.

(b) Include justification.

(c) Include the priority code according to AR 190-13, paragraph 4-9.

(d) State the Operations and Maintenance, Army (OMA), funds necessary to reimburse design, site preparation, and installation costs; and the Other Procurement, Army (OPA), funds necessary for “systems” equipment procurement.

(e) Include a consolidated equipment list that indicates by fiscal year the quantity of each piece of PSE required.

(3) Commanders will prioritize forecasted PSE requirements and coordinate with the servicing provost marshal office, DPW, director of resource management, and DOIM. ASG commanders will review, consolidate, and prioritize forecast requirements before submitting them to the USAREUR PM.

(4) Forecast submissions alone do not constitute approval for PSE.

(5) On annual forecasts, commanders will note previously forecasted projects no longer required, projects suspended until another fiscal year, and changes in funding or equipment requirements.

(6) ESSs should be programmed for replacement every 5 to 10 years after initial installation or the last life-cycle replacement date. The service life will vary from system to system. The servicing DPW or provost marshal office will determine the replacement date.

(7) Unforecasted PSE and ESS requirements affect forecasted projects and must be submitted through the OPM to obtain funding approval. A project request packet must be prepared according to paragraph 6-9. Submission of unfunded requirements must include documentation of extenuating circumstances that prevented forecasting.

b. Programming ESSs for New Construction or Major Renovation Projects.

(1) When a construction project requires an ESS, an estimate must be provided of the required installation funds as a line item on the DD Form 1391 submitted for approval. If ESS installation funds were omitted from DD Form 1391, a user-change request for the ESS must be submitted to the higher command.

(2) OPA funding requests will be included for the purchase of ESSs with other OPA funds.

c. Programming Installation Funds.

(1) Except for Military Construction, Army (MCA), projects, ESSs costing less than \$750,000 may be paid for with OMA funds. The purchase of ESSs in excess of \$750,000 must be paid for with OPA funds. For additions to an existing ESS or other changes after an initial installation has been completed, commanders will use or request OMA funds.

(2) Installations will request OMA funds to maintain ESSs.

(3) Commanders will ensure ESS acquisition, maintenance, and monitoring requirements are included in their annual funding submissions for their installation OMA forecast.

6-7. COORDINATION

a. Requests for the purchase, issue, lease, and lease renewal of nonstandard ESSs require approval by the USAREUR PM. Requests must be sent through the BSB and ASG provost marshal offices to the OPM, HQ USAREUR/7A (AEAPM-SO), Unit 29931, Bin 153, APO AE 09086-9931.

b. Requests to purchase or issue Army standard ESSs (such as the USAREUR standard ESS, the Integrated Commercial Intrusion Detection System (I-CIDS), or the Joint-Services Interior Intrusion Detection System (J-SIIDS)) do not require USAREUR PM approval.

c. Upgrades to the USAREUR standard ESS or adding to an existing ESS require only the approval of the local provost marshal and DPW.

d. When required, ESS engineering site surveys must be conducted and submitted to the USAREUR PM (AEAPM-SO) for review approval. Site surveys are required for nonstandard ESSs before final approval and funding. Servicing provost marshal staff will help with a site survey according to Technical Manual 5-853-4, appendix C, with the servicing—

(1) DPW to help complete the site survey (if required), to identify site-preparation requirements and associated costs, to coordinate follow-on maintenance, and to forecast associated maintenance-funding requirements.

(2) DOIM representative. The DOIM must be requested in writing to identify available communication media and coordinate systems-communication requirements.

(3) DOL. The DOL must be requested in writing to provide assistance with equipment procurement and property book accountability.

e. Extensive or complex ESS projects require the expertise and participation of qualified electronic security engineers to properly complete the survey and design. Requests for this assistance must be sent through the OPM, HQ USAREUR/7A (AEAPM-SO), Unit 29931, Bin 153, APO AE 09086-9931.

6-8. ESS ACQUISITION

a. According to AR 190-13, paragraph 4-7d(2), “MACOMs shall approve all requests for purchase, issue, lease, or lease renewal of nonstandard PSE. Commanders below Army MACOM level are specifically prohibited from approving such requests. This includes commercial IDSs, EECSS, and CCTV when they are used for surveillance or assessment purposes.”

b. Under no circumstances will commanders or DPWs procure or allow security technologies to be procured or installed without approval from the appropriate provost marshal. Provost marshals will review and process ESS request packets according to this regulation.

c. The OPM, in coordination with the USACE-Huntsville Center of Expertise for Intrusion Detection Systems, has adopted new USAREUR ESS standards. Specific system and technical information about these new standards can be obtained by contacting the USACE-Huntsville or the Security Operations Branch, OPM. No other systems will be procured or installed without prior review and approval according to AR 190-13, paragraph 4-7d(2); and this regulation, paragraph 6-9.

d. Add-ons (for example, adding a zone or camera) to previously approved and existing systems only require coordination with the DPW and approval of the servicing provost marshal office.

6-9. REQUESTS FOR NON-ARMY AND NON-USAREUR STANDARD ESSs

Requests for non-Army or non-USAREUR standard ESSs will be sent through the servicing BSB and ASG provost marshal office to the OPM, HQ USAREUR/7A (AEAPM-SO), Unit 29931, Bin 153, APO AE 09086-9931.

a. Requests for non-Army or non-USAREUR standard ESSs will include the following information:

- (1) A request for system approval and funding if required.
- (2) Cost estimates for purchase and installation if required.
- (3) A detailed plan on how the equipment or system will be used and operated.
- (4) A statement identifying the basis of submission and justification for the project.
- (5) Supporting documentation (for example, copies of PS inspections, surveys, or JSIVAs).
- (6) The designated security level of the facility or installation where the equipment will be used or installed.
- (7) Justification as to why Army or USAREUR standard ESS cannot meet requirements.
- (8) The project POC, telephone number, and e-mail address.
- (9) A description of and the desired or recommended source for the equipment.

b. In addition to the information in subparagraph a above, the following is required when requesting a new or major upgrade to an existing nonstandard, commercial ESS:

- (1) Justification as to why an existing ESS cannot be used by modifying or expanding its capabilities.
- (2) A completed site survey, technical specifications of proposed system and components, and engineer blueprints or drawings to scale of the system (protected area and component locations).

(3) Verification by the ASG commander that base operations (BASOPS) funds are available or have been programmed to maintain the system. The memorandum will not be forwarded unless BASOPS funds are available or have been programmed.

c. Figure 6-1 is a sample request for non-Army or non-USAREUR standard ESSs.

DEPARTMENT OF THE ARMY

REQUESTING UNIT

UNIT 00000

APO AE 00000-0000

OFFICE SYMBOL

Date

MEMORANDUM THRU:

BSB PROVOST MARSHAL (*for regulatory guidance and review*)

BSB DIRECTORATE OF PUBLIC WORKS (*for design and cost estimates*)

BSB DIRECTORATE OF INFORMATION MANAGEMENT (*for communication media*)

ASG PROVOST MARSHAL (*for final review ensuring proper staffing and format before final submission*)

ASG COMMANDER (*for verification that BASOPS funds are available or have been programmed to maintain the system*)

FOR: OFFICE OF THE PROVOST MARSHAL, HQ USAREUR/7A (AEAPM-SO), UNIT 29931, BIN 153, APO AE 09086-9931

SUBJECT: Request for Non-Army/Non-USAREUR Standard Electronic Security System (ESS)

1. Reference AE Regulation 190-13, paragraph 6-9, Requests for Non-Army and Non-USAREUR Standard ESSs.

2. Request approval for installation of an electronic security system for the *Unit, Type Facility, or room*, located in building *0000* on *local installation/casern, city, country*. The designated security level of this facility is ____.

3. *Brief statement identifying the basis for project submission (for example, to meet regulatory requirements, reduce vulnerability identified during risk analysis or security survey, or to reduce manpower requirements). Other supporting basis for installing commercial systems may be to expand or remain compatible with existing commercial systems.*

4. *Statement of justification explaining why Army or USAREUR standard ESS cannot meet requirements (for example, cannot integrate CCTV or electronic access control, installation is cost-prohibitive, distance from secure area to monitoring station is too far to establish direct communications). Include details on manpower or cost savings (for example, how much or how many).*

5. *Operation plan: Describe how the system will be deployed and operated (for example, who will monitor and where will it be located). Briefly describe how the system operates.*

6. Maintenance plan: *Describe the plan for maintaining the system and if BASOPS funds have been programmed and are available for maintaining the system.*

7. In accordance with U.S. Army Corps of Engineers Site Survey Procedures Guide for Electronic Security Systems, the ____ ASG/BSB Physical Security Office conducted a site survey in conjunction with the ____ BSB Physical Security Inspector, ASG or BSB DPW, and DOIM personnel as indicated on the Engineering Survey.

8. Projected fiscal year for installation is FY ____ subject to available funding.

9. The *ASG or BSB* Provost Marshal POC is *name*, DSN *telephone number*.

FOR THE COMMANDER:

5 Encls

SIGNATURE BLOCK

1. Engineering Site Survey (*Complete*) (*Technical Manual 5-853-4*)
2. Technical Specifications of Proposed Components
3. Equipment List and Cost Estimate
4. Digital Photos for Visual Support (*Recommended but not required*)
5. Other Supporting Documentation

Figure 6-1. Sample Request for Non-Army or Non-USAREUR Standard ESS

6-10. ELECTRONIC SECURITY SYSTEMS

a. As defined in Technical Manual 5-853-4, ESSs include IDSs, CCTV, and EECSSs. These systems may be used to enhance a facility's PS posture. FM 3-19.30, chapter 6, provides information on ESSs and their recommended uses.

b. Only qualified electronic-security engineers, in coordination with PS personnel who have successfully completed the USACE Electronic Security Systems Design Course, will survey for and design ESSs in the European theater. When properly designed, installed, and maintained, ESS technologies can be a valuable addition to PS programs. The effective use of ESSs requires a "total system" approach that integrates policy, procedures, equipment, protective construction, and awareness. This requires a coordinated effort on the part of the requesting unit and the supporting provost marshal PS office, the DPW, and the DOIM.

c. A properly designed ESS can increase security while reducing guard requirements by providing remote-detection and assessment capabilities and by electronically controlling access to restricted areas.

d. Contractor-installed IDS and PSE systems will be inspected by trained or certified DPW personnel before the installed system is accepted. Performance criteria required for acceptance of commercial intrusion detection systems (CIDSs) and commercial security technologies will meet or exceed the criteria in applicable technical bulletins and technical manuals.

e. According to AR 190-13, paragraphs 4-13b and c, a post-completion evaluation of an ESS installation may be requested from the IDS Mandatory Center of Expertise, Huntsville, Alabama, to ensure that the ESS was properly installed and is being maintained at the appropriate level. This evaluation is required for ESS and other PSE projects using sophisticated technologies. Funding for this evaluation must be programmed through the USAREUR PM and will be included in OMA forecasts.

6-11. ESS PLANNING GUIDELINES

a. AR 190-13, paragraph 4-15, discusses planning for IDSs and other ESSs. These systems are planned, budgeted for, procured, and initiated the same as other Army systems. AR 190-13, paragraph 4-16; and this regulation, paragraph 6-9, provide information on project submission and acquisition procedures.

b. In general, ESS and IDS projects are initiated to—

- (1) Comply with regulatory requirements or design standards.
- (2) Correct a deficiency identified on a PS inspection or survey.
- (3) Consolidate alarm-monitoring services as an effort to conserve manpower.
- (4) Reduce vulnerabilities or threats identified during FP vulnerability assessments.
- (5) Use instead of guards as a means to ensure continuous surveillance or control access to a restricted area.
- (6) Meet security requirements identified during the design of MCA projects.

(7) Meet security requirements identified during the design of funded renovation projects. Such projects may require the programming of OPA funds if new equipment must be purchased.

6-12. INTRUSION DETECTION SYSTEMS

Specifications for constructing ESSs and IDSs are outlined in United States Army Corps of Engineers Guide Specification (CEGS) 13720 and 13721. IDSs will be designed according to CEGS 13720 and 13721 and comply with the minimum requirements outlined in AR 190-11, paragraph 3-6.

a. All protected areas will be protected by an IDS consisting of at least two types of sensors. One sensor must be a volumetric sensor. The other sensor must be a balanced magnetic switch mounted on the arms-room door. A duress (hold up) alarm component is also required.

b. The IDS must—

- (1) Include a central control station where alarms will sound and from which a response force can be dispatched.
- (2) Be designed so that an alarm sounds at the central control panel whenever the system is turned off or malfunctions.

c. The response force must be capable of responding to an alarm by arriving at the scene within 15 minutes.

d. Each protected area must have an IDS sign affixed at eye level on the outside of each exterior wall that has an entrance to the protected area.

e. The IDS must have a protected, independent, backup power supply that is capable of providing 24 hours of uninterrupted power to the system (4 hours if located on an installation).

f. Units and activities with IDSs in facilities located off installations and in the civilian community must arrange for alarms to be connected and monitored at a local host-nation police station or an MP station from which an immediate response can be directed. A dial-up or autodial system or commercial answering service is not authorized.

g. A daily log must be maintained of all alarms received using DA Form 4930-R or by electronic means. Information about the nature of the alarm, the date and time the alarm was received, and what action was taken in response to the alarm will be included in the log.

h. Transmission lines for alarm circuits must have line supervision. If these lines are not available, two independent means of alarm-signal transmission must be provided. Unsupervised IDS lines that travel outside the protected area must be protected by a rigid conduit.

- i. The IDS must be tested each month. A record of these tests must be kept for at least 1 year.

6-13. IDS OPERATING PROCEDURES

- a. The three basic modes of IDS operation are as follows:

(1) Secure/Armed. A system is in secure mode or armed when a protected area is secured or closed and the IDS sensors are active. Alarms (duress, intrusion, and tamper) are processed and routed to the status modules. Intrusion and tamper alarms are routed to an audible alarm, if used. With CIDSs, an exit-time delay of 45 seconds will be provided to allow authorized personnel to secure or arm the system and leave the protected area without setting off an alarm.

(2) Access/Disarmed. A system is in access mode or disarmed when a protected area is open to authorized personnel. When systems are in access mode or disarmed, the sensors are masked or set to prevent intrusion alarms from being routed to the status modules and an audible alarm. Duress and tamper alarms are routed to the status modules continuously. The duress alarm must be configured to be a silent and must not trigger a local, audible alarm. With CIDSs, an entrance-time delay of 30 seconds will be provided to allow authorized personnel to enter the protected area and turn the alarm system off or disarm it without triggering an alarm.

(3) Test/Reset. The test/reset mode on a J-SIIDS control panel is used when maintenance is being performed on a system. In this mode, sensors are set to prevent alarms from being routed to the audible alarm. (They are routed to status modules instead.) On receiving alarm input, an audible signal in the control unit is activated for 10 seconds as an aid to IDS testing. If the mode switch is placed momentarily in the test/reset position, the audible alarm is reset and silenced. When the mode switch is switched from the test/reset position to the secure position, all processed alarms are cleared if the sensor inputs have ceased to be alarmed.

- b. The monitor console operator and control unit operator will use duress procedures. Supervisory personnel will establish duress procedures for use at the IDS monitor location. Procedures should be changed at least quarterly or when a compromise in security is suspected. Only personnel authorized to access (disarm) or secure (arm) the protected area and monitor personnel will have knowledge of duress procedures.

- c. Intrusion alarms will annunciate (sound) at the monitoring station. A duress alarm has priority over all other alarms and will be relayed to response forces by the alarm monitor using the fastest means available (preferably direct voice communication). Monitoring stations or consoles will be located where a response force can be dispatched.

- d. Monitoring stations will be staffed continuously to ensure immediate response to alarm annunciations. Alarm-monitor personnel will not be assigned any additional type of duty that interferes with or distracts them from their ability to respond to alarms.

6-14. IDS TEST PROCEDURES

a. General.

(1) IDSs will be tested with the monitoring station each month. "Tested with the monitoring station" means that the alarm will be deliberately activated to determine if the sensors work properly and the monitoring station actually receives the signal.

(2) Tests will be coordinated in advance with the monitoring station, normally by telephone. Ideally, one individual will remain in telephone contact with the monitoring station while another actually performs the test.

(3) Test procedures will vary according to the type of IDS in use. Testing will be done by performing the activity that the IDS is designed to detect. Every sensor will be activated or tested. Specific guidance for common types is provided below.

(4) AR 190-11, appendix K, provide test procedures for the J-SIIDS.

b. IDS Devices. The following IDS devices will be tested as follows:

(1) Balanced Magnetic Switch (BMS). This sensor detects attempts to open the door.

- (a) Begin with the system turned on, and the door closed and latched.
- (b) Attempt to shake, bump, or rattle the door. The alarm should not activate.
- (c) Slowly open the door. The alarm should activate before the door has moved more than 1¼ inches; some systems may have slightly different specifications.

(2) Ultrasonic Motion Sensor (UMS) or Passive Infrared (PIR). These sensors detect motion within the vault. Vaults in the European theater normally have one or the other, but not both.

- (a) Begin with the system turned on, the door closed, and the testing individual inside the vault.
- (b) Slowly move through the area covered by the sensor. The alarm should activate.
- (c) Reset the system and repeat several times by moving in different directions, both walking and crawling or crouching, until coverage in all areas of the vault has been tested. Ensure each UMS or PIR has been tested.

(3) Passive Ultrasonic Sensor (PUS) or Shock Detector (SD). These sensors detect attempts to break through the vault wall. Few are installed in the European theater.

- (a) Begin with the system turned on, the door closed, and the testing individual outside the vault.
- (b) Using a hammer or similar object, tap the wall several times. The alarm should activate. However, the number of taps and the amount of force required will vary according to the system specifications.
- (c) Reset the system and repeat several times at different locations on each wall of the vault.

(4) Capacitance Proximity Sensor (CPS). This sensor is used only on class 5 containers in a substandard storage facility, normally as a substitute for a UMS or PIR. The CPS detects someone touching the container.

- (a) Begin with the system turned on, the door closed, and the testing individual inside the vault or arms room.
- (b) Attempt to touch the class 5 container. The alarm should activate as or slightly before the container is touched.
- (c) Reset the system and repeat with each container.

(5) Duress Sensor (DS). This sensor is used to advise the monitoring station that the individual accessing the vault is under duress (for example, being held up). There are a variety of such devices; testing procedures vary.

- (a) If the DS is a separate switch or button in the vault:
 - 1. Begin with the system turned off, the door open, and the testing individual in the vault.
 - 2. Push the button and move the switch. The alarm should activate, but only at the monitoring station.
 - 3. Reset the system and, if there are other DSs, repeat with each.
- (b) If the DS is a separate switch or button located outside the vault:
 - 1. Test as in (a) above, but with the testing individual at the IDS location.
 - 2. Repeat with the system turned on and the door closed.
- (c) If the DS is part of a touch-pad located in the vault that is used to turn the system on and off:
 - 1. Begin with the system turned on, the door closed, and the testing individual in the vault. Enter the code that will send a duress signal. The alarm should activate, but only at the monitoring station.

2. If the system is also capable of sending a duress signal after being turned off, reset, turn the system back on, and enter the normal access code. After the system is turned off, touch the appropriate buttons. The alarm should activate, but only at the monitoring station.

NOTE: Most touch-pad DS systems are designed to send an alarm as the system is turned off by varying the access code. Many will also allow an alarm to be sent after the system has been turned off by touching certain buttons.

c. Checklists.

(1) Commanders are encouraged to develop and require the use of testing checklists tailored to the specific IDS in use in their facilities. Checklists help guide the individual conducting the test and also provide a written record for the test.

(2) In some locations, facilities have IDSs protecting areas other than vaults and arms rooms (for example, perimeter IDSs and exterior IDSs to protect aircraft). Commanders should develop testing procedures and checklists for these systems using this chapter for general guidance.

6-15. JOINT-SERVICES INTERIOR INTRUSION DETECTION SYSTEM (J-SIIDS)

Since J-SIIDS is Army standard PSE, the BSB provost marshal will act as the approval authority for all requests for J-SIIDS. Requests for J-SIIDS must be coordinated with the servicing DPW, DOIM, and DOL.

a. The two categories for J-SIIDS requisition are initial issue and replacement. DA funds initial-issue components for use based on MACOM submissions in the 5-year forecast of requirements. Replacement components are not free-issue and requisitions must be in Military Standard Requisitioning and Issue Procedures (MILSTRIP) format according to AR 725-50 and forwarded to the source of supply for each IDS component item as listed in the Army Master Data File.

b. To receive an initial issue of J-SIIDS components free of charge, the requesting activity must send a request by memorandum through the servicing BSB provost marshal office to the OPM, HQ USAREUR/7A (AEAPM-SO), Unit 29931, Bin 153, APO AE 09086-9931.

(1) The request must include supporting documentation and copies of the completed requisition forms (DA Form 2765-1 or DD Form 1348-6) with the appropriate document numbers.

(2) Requisitions must be in MILSTRIP format according to AR 725-50. Supporting documentation will include a statement identifying the basis for project submission, a complete list of required components, a cost estimate for system installation, and supporting justification for the request (for example, PS inspections or surveys).

(3) The BSB PSO or NCO will send the request memorandum to the USAREUR PM (AEAPM-SO) by fax (DSN 381-8140) with a list of required components and copies of the completed requisition forms. The memorandum through the BSB provost marshal office serves as the official verification that the installation has been properly designed and approved.

c. When filling out requisition forms, the requesting activity must ensure that the proper NSN, quantities, and document numbers are filled in, along with the six-digit code for the supplementary address to identify where the equipment should be shipped. If the supplementary address is unknown, the receiving activity must provide a POC, DSN telephone number, and complete address to identify where the equipment should be shipped.

d. Requests for initial-issue IDS components will be sent by mail or fax to the United States Army Communications - Electronics Command (AMSEL-LC-IEW-R-GS), Building 1201 West, 1st Floor, Fort Monmouth, NJ 07703-5000; fax DSN (312) 987-5880.

e. Users of Government-furnished equipment will maintain approval documents, requisitioning information (such as complete requisition numbers, the date of order, and a list of components), and any other information necessary to track the procurement process effectively. Requesters will make periodic checks with their servicing DOL to check the status of ordered equipment.

6-16. ALARM MONITORING GROUP AND INTEGRATED COMMERCIAL INTRUSION DETECTION SYSTEMS

a. The Office of the PM-PSE, United States Army Communications - Electronics Command, Europe, centrally manages the Alarm Monitoring Group (AMG) and I-CIDS programs. These systems are Army standard PSE; therefore, commanders do not require approval from the USAREUR PM to install and use them.

b. The J-SIIDS and the AMG are being eliminated and must be replaced with an I-CIDS or the USAREUR-approved standard commercial system. Requests to be added to the I-CIDS fielding list must be sent through the servicing BSB and ASG provost marshal office to the USAREUR PM. The USAREUR PM will consolidate requests to be added to the I-CIDS fielding list and forward the requests to HQDA and PM-PSE.

6-17. COMMERCIAL INTRUSION DETECTION SYSTEMS

CIDSs are commercially developed and manufactured IDSs that are considered non-Army and non-USAREUR Standard PSE. The requirements for procuring these systems are outlined in paragraph 6-9.

6-18. CLOSED-CIRCUIT TELEVISION (CCTV)

Specifications for constructing CCTV systems are outlined in CEGS 16751. Specifications for constructing exterior security lighting and CCTV applications are outlined in CEGS 16528. The requirements for procuring these systems are outlined in paragraph 6-9.

a. CCTV—

(1) May be installed when interfacing with existing or planned IDSs as an alarm-assessment tool.

(2) Generally may not be installed for surveillance purposes. CCTV may be used at ACPs to record personnel and vehicles entering the installation for investigative purposes.

(3) Must be connected to a recording device and recording at all times when used.

b. Commanders are encouraged to use digitized systems where the images are stored on hard-disk media instead of storing captured video on tapes that must be continuously rotated to preserve the images.

c. Commanders are prohibited from using CCTV and other EECSs for time-and-attendance purposes.

6-19. ELECTRONIC ENTRY/ACCESS CONTROL SYSTEMS

Specifications for constructing EECSs are outlined in CEGS 13720. The requirement for using EECS to control access to classified information is in AR 380-5, chapter 7. The requirements for procuring these systems are outlined in this regulation, paragraph 6-9.

a. All newly acquired EECSs in the Army in Europe will use contactless “proximity” technology.

b. Card-swipe and magnetic-strip type reading devices will no longer be approved for use with Army EECSs. Current owners and operators of systems that use these types of readers for controlling access to controlled or restricted areas will replace them by 1 October 2003.

c. All newly acquired or upgraded EECSs will be equipped with a minimum of 12-hour battery backup.

d. All systems must be approved by the USAREUR PM and local fire and safety officials before and after installation. Fire and safety officials will ensure that the system has life safety features built in.

e. The DOD common access card (CAC) and other contactless cards approved by the USAREUR PM may be used for electronic key access to facilities that are not classified as restricted areas. The CAC will not be used as a security badge for access to restricted areas.

f. According to AR 190-13, chapter 5, security identification cards and badges to control movement into and within restricted areas must—

(1) Identify the name of the installation or activity for which they are valid.

(2) Show the name and photograph of the person to whom the card or badge is issued. Visitor cards and badges will show "Visitor" in place of name and photograph, and will have "Escort Required" or "No Escort Required" printed across the face of the badge as appropriate.

(3) Have a serial number.

(4) Show an expiration date if issued for restricted (limited and exclusion) areas.

(5) Identify the areas for which they are valid.

g. When used as an electronic entry/access control card to enter restricted areas, the CAC and other approved electronic-access cards will be treated in the same manner as keys and accounted for at all times. All users of key cards will acknowledge in writing their responsibilities for securing and safeguarding their key card.

h. Electronic locks or door strikes may be used to control access to restricted areas during duty hours. After duty hours, restricted areas must be secured using manual, key-operated locks or combination locks as required.

i. All new purchases of blank cards for use with an EECS controlling access to restricted areas will have serial numbers.

j. An accurate, written record or log will be maintained to provide a documented audit trail from the time the blank badge cards are received or fabricated.

k. Previously procured or issued badges that do not have a serial number may be used until supplies are exhausted.

6-20. ESS/IDS KEY CONTROL

a. During the initial installation and test phase of the ESS, the installing activity will maintain key control. On completion of the final test and acceptance of the ESS, control and accountability of ESS keys become the responsibility of the unit or activity commander. Keys will be controlled according to AR 190-11, paragraph 3-8; and AR 190-51, appendix E.

b. ESS and IDS keys must be stored separately from administrative keys. These keys must be accessible only to those individuals whose official duties require access.

c. A roster of persons authorized access to ESS keys must be maintained and protected from view. This roster may be the same as the one prepared for AA&E access.

d. Keys required for maintaining ESSs must be kept separate from other ESS and administrative keys.

e. For AA&E storage areas, the IDS key and day gate key must be placed on a separate ring from AA&E keys, but may be left in the same storage container.

6-21. ESS/IDS PERSONAL IDENTIFICATION NUMBERS

Personal identification numbers (PINs)—

a. May be used to activate or deactivate an alarm panel or used to gain access to restricted areas.

b. Must not be shared or written down in locations where others have access.

c. Must never be used twice by the same organization.

d. Must be changed at least once a year. PINs must also be changed when the individual assigned the PIN no longer requires access or if there is reason to suspect that the PIN was compromised.

6-22. PHYSICAL SECURITY PLANS

Provost marshals will ensure that installation PS plans provide detailed instructions on the following:

a. ESS and IDS monitoring procedures.

b. Response-force procedures.

c. ESS and IDS testing and inspection requirements.

d. Actions to be taken in the event of power failure, and the identification of auxiliary power sources.

6-23. MAINTENANCE OF ESS

a. Commanders will ensure that only trained and qualified personnel maintain ESSs and IDSs.

b. Trained or certified DPW personnel may perform maintenance on ESSs unless maintenance is to be performed by contract. Local national contractors must have a completed foreign national screening with no derogatory information to perform maintenance on ESSs. At no time will an uncleared, non-U.S. citizen perform any type of maintenance on systems providing protection for SCIFs.

c. The DPW is responsible for maintaining ESS drawings, providing copies of drawings to the using activity, and updating drawings when changes occur.

d. Unit-level maintenance of ESSs is restricted to general cleaning-type maintenance (for example, dusting and wiping the exterior of IDS components with a dry cloth). IDS components will not be painted.

e. Contractor-installed ESSs will be maintained as specified in the Government maintenance contract. The contractor should be required to perform routine maintenance inspections at least every 6 months.

f. The time for responding to requests for maintenance of IDSs must be no longer than 24 hours during the week or on the next business day if a problem is discovered on a weekend or holiday.

6-24. PERSONNEL SUITABILITY AND RELIABILITY CHECKS

a. Requirements for personnel suitability checks and clearances for PSE installation and maintenance will be clearly stated in contracts.

b. Commanders may develop command-oriented background-check requirements consistent with the local threat situation, the sensitivity of the facilities protected, and the vulnerability of the facilities served.

c. U.S. personnel whose duties will involve designing, operating, monitoring, or maintaining ESSs or IDSs must have a favorable national agency check (NAC) or national agency check and written inquiries (NACI).

d. When the duties of local national employees or contract personnel involve designing, operating, monitoring, or maintaining ESSs or IDSs, these personnel must be processed through the Foreign National Screening Program according to USAREUR Regulation 604-1 and must not have any derogatory information on file.

e. USACIDC special agents may be available to conduct proper personnel background checks (criminal record verification) on personnel who have access to protected or restricted areas. This assistance may be received by written request to the local supporting USACIDC resident agency.

6-25. MOVEMENT OF ESS COMPONENTS AND SYSTEMS

a. ESSs will not be activated, deactivated, or moved without written notification to the servicing provost marshal office and DPW.

b. Activity and facility closures, organization moves, and inactivations may invalidate the need for certain ESSs. Commanders, in coordination with the supporting DPW, will identify inactive ESSs that may be laterally transferred to other locations. ESS components removed from closing installations will be turned in to installation property book officers. Installations may keep removed components, if needed, to backfill outstanding requisitions or to fill maintenance-float densities. The disposition of excess components will be coordinated through the DOL. Enough planning must be done to program for the ESS contractor to remove or install a zone without invalidating existing warranties.

6-26. IDS INSPECTIONS

PSIs will—

- a. Conduct an IDS check during security inspections and surveys.
- b. Conduct operations and functions inspections of IDS during scheduled PS surveys and inspections to ensure sensors, signal processors, control units, and monitor consoles and cabinets work. PSIs will use available operator manuals.
- c. Visually inspect components and conduits for evidence of tampering.
- d. Review engineer drawings of the various zones to ensure sensor and control unit locations are as indicated on the drawings.
- e. Ensure sensors are positioned in locations that provide maximum coverage of the protected area.
- f. Ensure enough sensors are used without operating the sensors at maximum sensitivity.
- g. Ensure the control unit is mounted on the interior wall of the protected area as close as possible to the main entrance to the protected area (except for class 5 weapons containers).
- h. Ensure the monitor cabinet or system is not obstructed from the continual view of monitor personnel.
- i. Ensure a duress alarm (commercial or J-SIIDS alarm latching switch) is positioned inside the protected area in a location where it is readily accessible to duty personnel and can be operated without being observed by an intruder.
- j. When installed at designated sites, the audible alarm will be located on the outside of the protected area and mounted as high as possible on the protected structure wall or utility poles. This will prevent tampering and increase the sound effect. The audible alarm must be accessible to maintenance personnel.

NOTE: Alarm systems using audible alarms must be configured so an audible alarm does not sound when a duress switch is pushed or a code is entered into the keypad.

6-27. ACCESS ROSTERS

- a. A roster of personnel authorized to disarm and arm the protected-area IDS will be provided to the monitor station. The roster will indicate the name, social security number, and telephone number of personnel at the protected area. The commander of the protected area will sign the roster. The roster will be kept where it is readily available to the monitor station operator and out of sight of unauthorized personnel.
- b. BSB PSOs will obtain the list of trained and qualified PSE and ESS equipment installation and maintenance personnel from appropriate activities, verify that their security screening has been completed, and provide this list to the monitor station and unit or activities with protected areas. The BSB PSO will verify and authenticate the roster.
- c. The roster will indicate the name, social security number, security clearance or background and records check as applicable, and telephone number of authorized personnel. Only personnel who have had favorable checks will be included on the roster. To prevent unauthorized tampering with the IDS, only personnel listed on this roster will be permitted to perform maintenance.

6-28. RESPONSE TO ALARMS

- a. Commanders or provost marshals will establish alarm-response policy and procedures. Policy implemented through local FP and crisis management plans must designate the response-force type, size, and armament.
- b. Installation commanders or provost marshals will establish procedures on the use of force according to AR 190-14.

CHAPTER 7 USAREUR CONTRACT GUARD PROGRAM

7-1. PURPOSE

This chapter—

- a. Supplements the requirements of AR 190-56.

b. Assigns responsibilities and prescribes policy, standards, and procedures for using military and civilian guard forces in the Army in Europe.

7-2. APPLICABILITY

This chapter applies to units in the Army in Europe, guards hired through CPACs, and contract guards. Commanders will consider local laws, international and host-nation agreements, the Status of Forces Agreement (SOFA), tariff agreements, and contract provisions when implementing the policy and procedures of AR 190-56 and this regulation.

7-3. OBJECTIVES

The objective of the USAREUR Contract Guard Program is to provide a professional, high quality, and effective security guard force. It provides centralized direction while ensuring the commander retains the responsibility to manage local personnel and assets.

7-4. GUARD AUTHORITY

The authority for guards is based on the SOFA, host-nation laws, and AR 190-56. USAREUR Regulation 525-13 provides additional information.

7-5. TYPES OF GUARDS

a. MP. The MP may be used to guard critical and sensitive facilities and activities as determined by the ASG commander according to USAREUR Regulation 190-62. With few exceptions, the MP will be used as guards only when specifically authorized by modification table of organization and equipment (MTOE) or table of distribution and allowances (TDA).

b. Contract Guards. Security services may be contracted through competitive bids. Contracted security services must comply with the USAREUR contract guard PWS and this regulation. The USAREUR contract guard PWS will be used as a model for developing contract-guard services in the European theater and modified only as required by host-nation laws or the SOFA. IMA-Europe or HQ USAREUR/7A will fund all contract-guard requirements to meet the regulatory and established, permanent USAREUR FP requirements. The USAREUR G8, however, may provide additional funding for emerging requirements above and beyond annual base program-funding levels provided through the Resource Management Office, IMA-Europe. Requesting organizations may be required to fund their requests for additional or temporary guard services, especially for positions that fall outside the scope of the base guard contract.

c. Borrowed Military Manpower. For the purpose of security-guard missions, BMM refers to soldiers used outside of their assigned military occupational specialty for specific security duties. This includes short-duration duties that do not technically qualify as BMM by strict definition. BMM will be used when other types of guard forces are neither available nor appropriate for a particular security requirement. USAREUR Regulation 525-13 provides qualification and training requirements for BMM.

d. CPAC Guards. Locally hired civilians (DA and local national) may be authorized on a TDA and hired through the local CPAC to work as guards. The use of CPAC guards is discouraged. Currently no CPAC guards are being used in the European theater.

7-6. POLICY

Guards are a valuable resource. They may be used either in an active capacity (for access control) or in a passive role (for surveillance and detection). Since guards are a valued asset, they should be used only where alternate solutions are not practical or allowable and when the risk to the protected asset warrants such protection. Because of manpower and funding constraints, guards will be provided only to the level essential to meet minimum-security standards. Security managers should seek reasonable alternatives, such as technology (for example, ESSs), instead of the long-term use of guards.

7-7. SELECTION, QUALIFICATION, AND SECURITY SCREENING OF GUARDS

a. General. AR 190-56 provides guidance on the standards for civilian guards. Qualification standards and security screening procedures for CPAC guards will be as specified in that regulation. Compliance with these requirements for contract guards will be accomplished as outlined below. Waivers to these requirements may be authorized only by the USAREUR PM.

b. Qualification Standards. The standards for contract guards in Germany are outlined in the USAREUR contract guard PWS. These include but are not limited to standards regarding character, age, experience, physical and mental fitness, nationality, and training. These standards will be modified as required by the SOFA, host-nation law, and operational factors.

c. Security Screening Procedures. All guards will have the appropriate extended (full) background check completed as indicated below before they are allowed to perform guard duties.

(1) Local National Personnel. Host-nation police good conduct certificates (for example, *Polizeiliches Führungszeugnis* in Germany) must be presented by local national applicants on application for employment with the contractor. These personnel will subsequently undergo a security check according to USAREUR Regulation 604-1 and other checks as deemed necessary and as stated in the USAREUR contract guard PWS.

(a) These requirements will be modified only as required by the SOFA and host-nation law in areas where the USAREUR contract guard PWS is not applicable. Changes to the USAREUR contract guard PWS not required by host-nation law or the SOFA will be forwarded to the USAREUR PM (AEAPM-SO) for approval. A favorable background investigation according to USAREUR Regulation 604-1 (or equivalent where Laredo Leader is not applicable) must be returned before a guard candidate may perform guard duties.

(b) In areas where checks according to USAREUR Regulation 604-1 may not be completed, the unit or organization preparing the USAREUR contract guard PWS will ensure that the best security-screening procedure is used to screen guard personnel used under the provisions of the USAREUR contract guard PWS.

(2) U.S. Personnel. U.S. personnel hired as contract guards will be screened using a combination of records checks from the provost marshal office in the community in which they reside and more extensive checks through the Defense Central Intelligence Index (DCII), National Crime Information Center (NCIC), and other checks as deemed necessary and as stated in the USAREUR contract guard PWS.

(3) Waivers. Waivers to the screening requirement require approval by the USAREUR PM. This approval will be based on the following conditions:

(a) The guard candidate must be properly trained and certified according to the basic requirements in the contract guard PWS under which he or she will be used.

(b) The guard candidate must be a native-born citizen of a NATO member country. The use of non-NATO personnel to guard U.S. Forces installations require approval by the CG, USAREUR/7A, or the DCG/CofS, USAREUR/7A.

(c) The guard candidate must have a completed host-nation police good conduct certificate or the equivalent.

(d) An extended background check on the guard candidate is at the appropriate intelligence agency for processing. Guard candidates waiting for the extended background check to be completed will only work with cleared personnel (for example, they may not work one-person guard posts).

d. Medical Examinations. Contract guards will take a medical examination when they apply for employment and be reexamined annually. The examining physician will verify the individual's physical and mental fitness to perform duties as a security guard. The local national surveillance contract administered by the preventive medicine department of U.S. Army medical facilities will be used to screen and evaluate medical records of CPAC guards.

e. Drug Screening.

(1) CPAC security guards are exempt from the Civilian Employee Drug Abuse Testing Program until this testing is approved by Army in Europe policy.

(2) All contracts for security guard services will include provisions for drug-abuse testing of guard personnel.

(a) Contract guards will be tested on initial employment, randomly as outlined in the contract guard PWS, and if they are suspected to be under the influence of alcohol or drugs while on duty. The testing will be conducted as an adjunct to the Army in Europe drug-testing program and will be in compliance with host-nation law. Samples will be submitted to and tested by Government agencies responsible for the Drug-Abuse Testing Program. Testing for alcohol may be done with the local provost marshal office and host-nation police.

(b) In areas where the testing of personnel is legally permissible but the Government testing program is not available, provisions will be made to test personnel at local medical facilities.

(c) Personnel testing positive for banned substances will not be allowed to work under the provisions of the USAREUR contract guard PWS.

7-8. INDIVIDUAL RELIABILITY PROGRAM

a. General. As outlined in AR 190-56, the Individual Reliability Program (IRP) is designed to ensure the initial and continued reliability and suitability of personnel to perform security duties. It assesses data derived from actions taken during the selection, qualification, and security screening of guards, as well as from the guard's duty performance and supervisor observations. Commanders are responsible for establishing and maintaining a viable IRP for all of their security personnel according to the guidelines below.

(1) The actions and responsibilities established in AR 190-56 will be followed when using CPAC guards. The execution of this program for contract guards will be as described below and according to the appropriate provisions included in the contract guard PWS. The contract provisions will be so as to obtain contractor compliance with the actions required of the organization to ensure the proper execution of the IRP.

(2) For contracts executed outside of the ASG structure (for example, for deployed task forces), before solicitation of the contract, the USAREUR requiring activity will forward a memorandum to the USAREUR OM that outlines the actions to be taken to comply with this regulation.

b. Certifying Official. AR 190-56 states that the IRP certifying official will be the commander or designated representative who is charged with the maintenance of law and order at an installation or facility.

(1) The commander may designate the provost marshal, security officer, or civilian personnel officer as the IRP certifying official. If so designated, the provost marshal may further delegate this function to a senior individual in the provost marshal office or security office.

(2) In the European theater, ASG commanders are designated as IRP certifying officials responsible for assessing the initial and continued reliability and suitability of contractor personnel to perform guard duties.

(a) The ASG commander will designate the ASG provost marshal as the IRP certifying official. The provost marshal will further delegate this function to the COR responsible for direct oversight of security guard contracts outside of Germany, or SCORs for contracts in Germany.

(b) The principal IRP certification official will maintain enough oversight over COR and SCOR activities to ensure the proper functioning and execution of the IRP.

c. Reliability Factors. The factors in AR 190-56, paragraphs 3-6 and 3-7, will be applied when assessing an individual's reliability to perform guard duties. These factors will be included in the contract guard PWS.

(1) Initial and Annual Evaluations. The initial evaluation by the COR or SCOR will be done using the results of the security and drug screening as well as the medical examination of the individual. Subsequent reviews (within 1 year after the initial evaluation) will include work performance and any required updates or renewals of screening and examination requirements (for example, updated good conduct certificates, annual medical examination).

(2) Continuous Evaluation. The contract guard PWS will—

(a) Include provisions requiring contractors to ensure that their personnel are responsible for reporting behavior and incidents affecting the reliability of their coworkers to their supervisors.

(b) Require that contractor supervisors at all levels be aware that they have an inherent responsibility to inform their supervisory chain of all incidents of erratic performance and poor judgment by personnel on or off duty that could affect on-the-job reliability.

(c) Require the contractor to report incidents of erratic performance and poor judgment to the appropriate COR or SCOR. The incidents will be reported immediately but (when appropriate) the contractor will be allowed to conduct an investigation to ascertain the accuracy of the report.

(3) Removal From Work. The contract guard PWS will include provisions that require the contractor to remove from work any personnel disqualified under the IRP by the certification official.

d. Certifying Official's Evaluation.

(1) Initial Review. The contract guard PWS will include provisions that the contractor will prepare DA Form 5557-R on each employee to be assigned guard or supervisor duties under the provisions of the contract and forward the form to the COR or SCOR for evaluation. The COR or SCOR will review all screening and examination documents that are received from the contractor or through Government channels. If the employee is IRP-certified, the COR or SCOR will complete the form as indicated below and send the original to the contractor for placement in the employee's personnel file.

(2) Completion of DA Form 5557-R. DA Form 5557-R will be completed when an individual enters the guard force and then annually thereafter. The contractor will maintain each completed form in the individual's personnel file and a copy will be maintained by the COR or SCOR. The form will be completed as follows:

(a) Part I - Personnel Records Screening: The contractor will complete the blocks for the employee's name. The designation *Guard* or *Supervisor* will be entered in the "grade" block, and the employee's company identification or badge number will be entered in the "SSN" block. The COR or SCOR will annotate the results of the background screening in the blocks that follow by indicating whether information *is* or *is not* attached (which may prevent assignment). The blocks on the type of security clearances will not be completed. The COR or SCOR will then complete the signature block (Name and Grade of Official Conducting Screening) and sign and date the form.

(b) Part II - Medical Records Screening: The COR or SCOR will review the results of the doctor's certificate, annotate the appropriate information blocks, place *REVIEWED* in the block for the physician's name, then sign and date the form.

(c) Part III - Certifying Official's Evaluation: The COR or SCOR will check the appropriate boxes, enter his or her signature block, and sign and date the form.

(d) Part IV - Briefing Certificate: The contractor will have the employee sign and date the form after the required briefing is provided to the employee.

(e) Part V - Disqualification: The COR, SCOR, or contractor will complete the appropriate entries as required if an employee is initially denied IRP certification or is subsequently removed from the contract because of IRP disqualification.

e. Retention for Reliable Duty Performance. When despite the presence of disqualifying factors an individual is kept because of overriding evidence of reliable performance of duty, the following actions will occur:

(1) The contractor will provide a written memorandum to the appropriate COR or SCOR requesting the retention of the individual and providing the reasons why the request for retention should be approved.

(2) The COR or SCOR will respond to the contractor approving or disapproving the request and include the rationale for the decision.

(3) The COR or SCOR will keep a copy of the complete correspondence and the contractor will place a copy in the employee's personnel file.

(4) Issues surrounding the retention or non-retention of personnel will be resolved at the lowest level of contract oversight starting with the SCOR, then the contractor's area or site manager, the COR, the project manager, and finally the contracting officer.

7-9. TRAINING

a. AR 190-56, chapter 4, provides guidance on guard training. All guards, regardless of their source, will be formally trained in their duties before performing security functions. USAREUR contract guards will be trained by the contractor according to the contract guard PWS. BMM guards will be trained according to USAREUR Regulation 525-13. USAREUR-specific contract-guard training requirements and standards are designated in the contract guard PWS.

b. The items in (1) through (9) below are minimum training requirements for all security guards. These are in addition to the requirements in AR 190-56 and USAREUR Regulation 525-13 and will be included as training requirements in all PWSs for guard services.

(1) Countersurveillance Techniques. Terrorist and other sophisticated criminal elements usually conduct extensive reconnaissance and surveillance before executing an action. Guards must be alert to unusual persons watching protected assets and areas, and should immediately report suspicious activities to supervisors. The ASG or BSB will review counter surveillance instructions and training for adequacy.

(2) Duress Procedures. Each guard will be trained on duress procedures and situations that might require those procedures.

(3) First Aid. Security guards will receive a minimum level of instruction in first aid and basic lifesaving techniques. Qualified medical personnel should conduct the training.

(4) Guardpost Orders. Security guards will be trained in each aspect of their assigned duties. Other aspects of a guard's functions, such as access-control procedures for gate guards and building-security checks for roving security guards, must be included in the guard-training program.

(5) IRP. Security guards will be trained on the IRP according to paragraph 7-8 and AR 190-56.

(6) Personnel, Vehicle, and Material Control. Security guards will be trained to properly search vehicles, personnel, and material when assigned duties that require such action. Local provost marshal and staff judge advocate personnel should help give instruction on conducting searches.

(7) Physical Training. Supervisors will ensure security guards maintain an acceptable level of physical fitness so they can perform their assigned duties. Contract guards will meet the requirements of the USAREUR contract guard PWS. Civilian Support Group guards will comply with USAREUR Regulation 600-474. CPAC guards will meet the performance standards in their job description.

(8) Weapons Qualification. Security guards will qualify with their assigned weapons before they are assigned to security duty. The USAREUR contract guard PWS and applicable host-nation law will establish qualification standards for contract guards. All other guards will qualify according to appropriate regulatory requirements.

(9) Use of Force. The decision to arm guards will be governed by applicable PS standards established for the asset being guarded and be based on both USEUCOM and Army in Europe FP standards on arming security personnel.

(a) Contract guard use-of-force rules will be in strict compliance with the SOFA and host-nation laws. Contractors will provide a standard ROE for their guard personnel according to host-nation law, the SOFA, and USEUCOM- and Army in Europe-specific requirements for arming security personnel.

(b) The MP is governed by AR 190-14 for the use of force.

(c) Civilian Personnel Operations Center personnel will comply with the provisions of USAREUR Regulation 600-472 and USEUCOM and Army in Europe policy guidance.

(d) BMM performing security and FP duties will follow the USAREUR standard FP ROE.

c. All policy and procedures on the use of force will be coordinated with the supporting staff judge advocate before being implemented. In general, security guards will use force only if they cannot conduct their duties without it. If the use of force is necessary, only the minimum amount needed to resolve the situation will be used.

7-10. UNIFORM AND EQUIPMENT

a. AR 190-56, chapter 6, provides guidance on guard uniforms and equipment. USAREUR-specific contract-guard uniform requirements are explained in the contract guard PWS.

b. Commanders and supervisors will ensure security guards under their control are adequately clothed and equipped to perform assigned duties. Based on the nature of the position and responsibilities of security guards, specific equipment may be required for duty. Individual and supplemental equipment considerations include inclement weather and unusual terrain.

(1) Individual equipment includes at least the prescribed uniform (seasonal and climatic), the individual's weapon (when authorized), and other individual supplies needed to perform security guard duties.

(2) Supplemental equipment includes vehicles, communications equipment, and other accountable property required to perform security-guard duties.

(3) Uniform and equipment requirements will be included in guard service contracts.

7-11. ESTABLISHING AND MEETING REQUIREMENTS

a. Guard requirements are generated if the guards are required by law or regulation or if the commander, based on a risk analysis, determines that a valid and prudent need exists.

b. No standard method is available for determining the number of guard positions needed to secure a given asset. Local operational considerations, the vulnerability of the asset, and required duties will be considered when determining an acceptable minimum number of guards. AR 570-5 explains how to develop manpower standards.

c. After establishing valid guard requirements (b above), paragraph 7-5 will be used to determine the type of guards needed to meet requirements.

(1) The use of BMM must be approved according to local ASG procedures.

(2) The use of MP may be approved only by the ASG commander according to USAREUR Regulation 190-62.

(3) The use of CPAC guards must be approved by the Region Director, IMA-Europe.

(4) The ASG commander will initiate any new request for additional contract guards. The request will be in the form of a memorandum sent by the ASG commander to the USAREUR PM (for temporary requirements of under \$200,000) or through the USAREUR PM to the DCG/CofS, USAREUR/7A (for permanent positions or any temporary requirement of over \$200,000).

(a) Requests will include a summary of the reasons or rationale for the request. The USAREUR PM will validate each new request for additional contract-guard support and coordinate funding for each request with IMA-Europe. The USAREUR PM will coordinate each new request with other HQ USAREUR/7A staff offices as necessary to review the requirement.

(b) Requests should be forwarded by the ASG at least 30 days before the desired start-date of the services.

(c) Once validated, all new permanent contract-guard requirements will be forwarded with a USAREUR PM recommendation to the DCG/CofS, USAREUR/7A, for decision. Each guard-request packet will include the IMA-Europe recommendation based on the status of funds to support the new requirement.

d. CPAC guards must be placed on the organization's manpower-authorization documents. A current PS survey will be made available on request to IMA-Europe when that organization conducts organizational surveys or functional-area assessments of authorized guard positions.

e. After guard positions in an organization have been validated and funded, ASG commanders may require short-term guard use beyond the validated level, based on an increased FPCON or local operational necessity.

(1) A need for more guards than validated must be met by the ASG assets, normally with support from tenant units. Augmentation beyond the capability of the ASG and tenant units must be requested according to USAREUR Regulation 525-13.

(2) When long-term operational requirements indicate the need for an increase of validated guard requirements, the process in subparagraphs b through d above must be followed.

7-12. GUARD ORDERS

a. AR 190-56, paragraph 5-3, provides guidance on guard orders. For contract guards, the contract guard PWS will include the general orders applying to all like installations. The ASG or BSB will subsequently prepare special orders for each installation in their operational area.

b. Each guard post staffed by host-nation personnel must have clear, special orders prepared (as appropriate) by an ASG or BSB staff element or tenant unit. These orders will be in English and the host-nation language and either be translated by the Government agency responsible for the preparation of the orders or translated by the contractor and then certified as accurate by the responsible Government element. These orders will describe the scope of the guard post, functions to be performed, and parameters within which each guard will operate. Special orders will address each aspect of the guard's duties. Orders will include at least the following information:

(1) The AOR. Orders must specify the area for which the guard is responsible. Use of a detailed sketch will help clarify the limits of the installation.

(2) Use of Force. Contractors are responsible for ensuring their personnel are properly trained in the host-nation laws regarding the use of force (including deadly force). A summary of these provisions (provided by the contractor) must be available at each guard post and must be part of the special orders for the guard post.

(3) Equipment. Orders will specify a list of required equipment that includes items for operation in bad weather and darkness (para 7-11b). Responsibility for the use, maintenance, and accountability of property and individual items of equipment must be clearly explained.

(4) Supervisory Control. The supervisory chain must be defined. Conditions when a guard may be required to comply with instructions from personnel outside of their supervisory chain also must be clearly explained.

(5) Duress Instructions. Clear duress procedures must be prescribed for each guard post.

(6) Reports and Forms. Clear instructions for using reports and forms, when such are required, must be provided; samples must be provided to each guard post.

(7) Access Control. USAREUR access control policy according to AE Regulation 190-16, USAREUR FPCON guidance, and local policy regarding access control must be available at each ACP. The contractor is responsible for thoroughly training personnel on the policy and procedures.

(8) Special Instructions. Unique situations and requirements of a specific guard post must be clearly detailed in the guard post orders. This will include actions to be taken at each level of FPCON.

c. In addition to general and special orders, local commands will provide at each guard post a "pass on" book. The book will include nonpermanent information of operational necessity at the guard post. This information will include BOLOs, spot reports, and unclassified intelligence information. All information in the book will be regularly checked and its currency verified. The U.S. Government is responsible for providing and updating the book and the contractor is responsible for ensuring that the book is reviewed by members of the guard post on assuming their duties.

7-13. CONTRACTOR EXPLOSIVE DETECTOR DOGS

Contractor explosive detector dogs (EDDs) are used to augment the MWD EDD, primarily for conducting random antiterrorism measure (RAM) searches of vehicles and cargo at ACPs. The use of contractor EDDs may only be approved by the USAREUR PM. Unless otherwise approved by the USAREUR PM, the use of EDDs will be limited to vehicle and cargo searches. Except under critical circumstances or when approved by the USAREUR PM, contract EDDs will not be used to support operations and events related to HRP or bomb threats.

a. Contract EDDs will be trained by the contractors to USAREUR MWD EDD performance standards. Training will concentrate specifically on RAM-oriented searches, such a vehicle and cargo searches at ACPs.

b. Contract EDDs will be certified by the USAREUR PM MWD certification authority according to applicable DA and USAREUR MWD EDD certification standards and provisions of the contract guard PWS, as applicable. These certifications will concentrate on evaluating the EDD team's abilities while accomplishing its primary mission of vehicle and cargo searches.

7-14. CONTRACT GUARD QUALITY ASSURANCE PROGRAM

Regular, routine evaluations of security guard operations are essential to ensuring compliance with this regulation, the contract guard PWS, local policy, and guard post general and special orders. Each contract for guard services will include a quality-assurance plan for use in monitoring compliance by the contractor with the provisions of the contract. The contractor will also implement a quality-control plan to monitor his or her own performance.

a. The COR or SCOR will use the Contract Guard Quality Assurance SOP at <http://www.hqusareur.army.mil/opm/pubs.htm> when executing contract quality-assurance plans.

b. Surveillance of contractor work performance must be enough to provide a reasonable assurance that guard services for which payment is requested were performed according to the provisions of the contract. The COR or SCOR will certify contractor invoices before approval for payment. To accomplish this, CORs and SCORs will—

(1) As a minimum, randomly observe or monitor 50 percent of all scheduled training. Only the COR or SCOR will monitor training and verify contractors' compliance with PWS requirements. A record of COR and SCOR attendance at training sessions with any deficiencies noted and a report of corrective action from the contractor will be maintained on file and available for review.

(2) As a minimum, randomly inspect at least 33 percent of all contract guard posts over all shifts during each month so that 100 percent are inspected each quarter. Of the 33 percent, at least 10 percent will be performed by the COR or SCOR. The remaining checks may be conducted by other appropriate staff elements in the ASG or BSB (for example, MP, FP personnel, installation coordinators) to ensure that all guard posts are properly manned. A record of the inspections with any deficiencies noted and a report of corrective action taken by the contractor will be maintained on file and be available for review.

(3) As a minimum, randomly inspect at least 10 percent of contract-guard personnel files monthly. These files will be maintained by the contractor. The inspection will ensure that all guard personnel employed and listed on the current guard roster are properly trained, qualified, certified, and equipped according to the PWS. A record of the inspections with all deficiencies noted and a report of corrective action taken by the contractor will be maintained on file and be available for review.

(4) The contractor will complete a daily guard roster. The roster will show the actual daily guard post manning by guard post number, guard name, and badge number at each guard post during each shift. The COR or SCOR will use the daily guard roster as a tool to monitor if guard posts are being manned according to the PWS. As a minimum, the COR or SCOR will check at least 10 percent of daily guard roster entries against the actual guard post manning requirements for each billing and invoice period. A record of the guard-roster verification checks with all deficiencies noted and a report of corrective action taken by the contractor will be maintained on file and be available for review.

c. The COR or SCOR will keep written documentation to substantiate certifying contractor invoices for payment. All findings of noncompliance will be provided in writing to the contractor for immediate corrective action. The COR or SCOR will reconcile lost work hours and other noncompliance issues that affect payment to the contractor. Any lost work hours, substandard performance, and other nonperformance issues that cannot be resolved by the COR or SCOR will be forwarded to the contracting officer for immediate resolution. A written record of action taken to reconcile noncompliance issues will be kept on file.

d. Maintenance and disposition of COR and SCOR files will be according to AR 25-400-2. Files will be kept current and include at least the following:

- (1) Copy of the contract and modifications.
- (2) Copy of the quality-assurance surveillance plan and external COR or SCOR SOP.
- (3) Copy of all completed surveillance activity checklists, inspections reports, and a suspense file.
- (4) Contractor reports of corrective actions.
- (5) Copy of the COR or SCOR appointment letter or orders.
- (6) Copy of COR or SCOR training certificates.

- (7) Current guard post list.
- (8) Current list of active contract-guard personnel.
- (9) Current training schedule.
- (10) IRP certification file.
- (11) Security clearance and background checks and a suspense file.
- (12) A copy of all correspondence pertaining to the contract (internal and external initiated).
- (13) A copy of all external and internal audits and inspections of the contract-guard program.

e. The ASG or BSB provost marshal office, as the proponent for PS and law enforcement, will advise the S2/3, and FP officer on security guard policy. The provost marshal office and the S2/3 will help CORs and SCORs monitor contractor performance as indicated above.

CHAPTER 8

OPM SECURITY OPERATIONS STAFF-ASSISTANCE VISIT PROGRAM

8-1. PURPOSE

This chapter prescribes policy and assigns responsibility for developing and maintaining practical, economical, and effective SAV programs.

8-2. REFERENCES

Appendix A lists required and related publications and prescribed and referenced forms.

8-3. SECURITY OPERATIONS BRANCH

The Security Operations Branch, OPM (AEAPM-SO), is responsible for overall PS policy and programs in the European theater based on an analysis of the mission and known or anticipated requirements and threats. This responsibility extends to contingency operations and missions throughout the European theater.

8-4. SAV SCHEDULES

The Security Operations Branch will establish and coordinate SAV schedules (PS and contract guard) at least 6 months before the planned SAV. SAVs will be conducted at ASG-, BSB-, and centralized installation management (CIM)-levels as appropriate or as determined by findings during SAVs.

8-5. PHYSICAL SECURITY SAV

The Security Operations Branch is responsible for conducting SAVs specifically addressing the Army in Europe Physical Security Program. This is in addition to PS inspections required by AR 190-13 and AR 190-16. A credentialed PSI will conduct all SAVs. Findings will be presented to the Physical Security Program Manager and the Chief, Security Operations Branch, for further action.

8-6. USAREUR CONTRACT GUARD SAV

The Security Operations Branch is responsible for conducting SAVs specifically addressing the USAREUR Contract Guard Program. Security Operations Branch personnel familiar with the Army in Europe Force Protection Program, the Army in Europe Physical Security Program, and the USAREUR Contract Guard Program will conduct these SAVs. The intent of the contract-guard SAV is to identify programmatic discrepancies between ASG, BSB, or CIM contract-guard programs. SAVs will also identify contractual discrepancies and report all findings to the USAREUR Contract Guard COR and the Chief, Security Operations Branch, for further action.

8-7. INTENTION OF SAV PROGRAM

The intention of the SAV program is to identify shortfalls and strengths of the Army in Europe Physical Security Program or Contract Guard Program. Through shared information, the overall security posture of U.S. Forces in the Army in Europe will be greatly enhanced. SAV programs will identify, document, and report installations or activities that require special PS or contract guard considerations because of their mission-essential or critical status and vulnerability to—

- a. Criminal acts.

- b. Dissidence.
- c. Hostile intelligence activities.
- d. Terrorist acts.
- e. Other disruptive influences.

8-8. REQUIRED SAV ACTIONS (PHYSICAL SECURITY)

During SAVs, the USAREUR PM representative will check the PS plan and all appendixes. The plan will be evaluated for its overall effectiveness. As a minimum, annexes to the plan that are required to be checked will include the following:

- a. Bomb-threat plan.
- b. Civil-disturbance plan.
- c. Communications plan.
- d. Complete list of MEVAs.
- e. Installation-threat statement.
- f. List of designated restricted areas.
- g. Natural-disaster plan.
- h. Resource plan.
- i. Terrorism counteraction plan.

8-9. REQUIRED SAV ACTIONS (CONTRACT GUARD PROGRAM)

During SAVs, the USAREUR PM representative will check the overall compliance with the current contract describing the USAREUR Contract Guard Program.

8-10. REPORT FORMAT

- a. SAV reports will be in a memorandum format and include the following:

- (1) Observations.
- (2) Discussion.
- (3) Options.

b. All observations will reference the regulatory or contractual requirement when appropriate. Any identified requirement will immediately be reported to the appropriate unit representative before the completion of the SAV.

CHAPTER 9

SECURITY EQUIPMENT WORKING GROUP (SEWG)

9-1. GENERAL

This chapter outlines responsibilities and provides guidance for the procurement of nonstandard, commercial FP/PS equipment. In addition, it provides policy guidance and procedures for the SEWG.

9-2. POLICY

The SEWG was established in October 2001 by order of the DCG, USAREUR/7A, to act as the USAREUR single POC for research, review, and procurement policy guidance for all FP/PS equipment.

a. Technological advances and limited resources require commanders to be prudent in assessment and selection practices. Because of numerous technological advances, a wide variety of commercial FP/PS equipment is available to enhance security postures throughout the European theater.

b. The SEWG was formed to act as the central POC for all security-related equipment in an effort to provide commanders with sound recommendations on the types of security equipment available to reduce identified vulnerabilities, as well as to provide recommendations for specific manufacturers and model numbers if they want to procure specific security hardware items.

c. This program addresses nonstandard, commercial FP/PS equipment only (para 9-3). Commanders may continue to procure standard FP/PS equipment without contacting the SEWG. Commanders are also authorized to procure equipment to supplement or maintain existing approved systems.

d. The intent of this regulation is not to limit commanders, but to avoid the need for each commander to make independent market analyses, operational evaluations, and other resource-intensive actions to select the best system to accomplish the mission. Additionally, equipment and technology throughout the Army in Europe can be standardized, which will facilitate economic initial procurement; operator training; maintenance, procurement, stockage, and distribution of repair parts and expendable supplies; and contractor logistics support arenas. To be effective, SEWG review processes must include a review of the detailed plan for use of the proposed nonstandard equipment. The SEWG can provide assistance by reviewing the commander's detailed implementation plan.

9-3. DEFINITION OF NONSTANDARD EQUIPMENT

Nonstandard FP/PS equipment for the purpose of this regulation is categorized in the following groups:

a. Communications or information-management equipment intended for FP/PS use.

b. Explosive-detection and chemical-detection equipment.

c. Metal-detection equipment that uses x ray technology.

d. Mechanical or electronic high-speed vehicle-barrier systems.

e. Mechanical or electronic personnel and vehicle-access-control systems.

f. Night-vision equipment intended for FP/PS use.

g. Nonstandard security equipment listed in AR 190-13, paragraph 4-7d(2). This includes CIDSs, EECSSs, and CCTV systems used for surveillance or threat assessments. AR 190-13 prohibits commanders below MACOM level from approving requests to purchase, issue, replace, lease, or renew leases for nonstandard PSE.

h. Mass-notifications systems.

i. Vehicle-inspection equipment.

j. Vehicle-tracking systems and devices.

9-4. SEWG RESPONSIBILITIES

a. The USAREUR PM will chair the SEWG. The membership of the SEWG will consist of selected representatives of the command.

b. The SEWG chairperson may establish subordinate working or advisory groups to address specific functional areas. These groups will be established by charter and disestablished when the group's function is no longer required.

c. Specific functions of the SEWG are to—

(1) Act as the single POC (clearinghouse) for nonstandard, commercial FP/PS equipment.

(2) Conduct research and collect data concerning performance specifications and published test results for nonstandard, commercial FP/PS equipment systems. Also validate (or refute) manufacturer's performance claims found in advertising and marketing literature.

(3) Provide a resource database to users of DOD-approved systems and systems considered viable by the SEWG.

(4) Provide a mechanism to consolidate and standardize requests for FP/PS equipment throughout the Army in Europe. Also conduct formal operational evaluations of FP/PS hardware to document performance capabilities and limitations.

9-5. PROGRAM MANAGEMENT

a. The SEWG will—

(1) Serve as the single POC for validating FP/PS equipment in coordination with the Office of the Science Adviser, HQ USAREUR/7A; and the Force Protection Division, Office of the G3, HQ USAREUR/7A.

(2) Coordinate with the following as required:

(a) Office of the G1, HQ USAREUR/7A.

(b) Office of the G2, HQ USAREUR/7A.

(c) Office of the G6, HQ USAREUR/7A.

(d) Office of the G8, HQ USAREUR/7A.

(e) Engineering Division, IMA-Europe.

(3) Ensure that only effective FP/PS equipment is recommended for procurement and use in the Army in Europe. Also continually review emerging technology with DOD and DA security equipment organizations.

(4) Coordinate issues concerning communication systems, vehicle-tracking systems, and microwave technologies with the USAREUR G6.

(5) Coordinate with other staff agencies as needed to ensure maximum cooperation and compliance to regulations and policy.

b. Commanders will—

(1) Ensure that all requests for procurement of commercial, nonstandard FP/PS equipment in paragraph 9-3 are coordinated with the USAREUR PM. A detailed plan of how the proposed equipment is to be used must accompany the request. The plan will include schematics and detailed information about how the technology will be used and what threat it is intended to defeat. (In other words, the request must describe the user requirement.)

NOTE: A list of all technology that has been considered and recommended for procurement by the SEWG is available on the USAREUR G3 webpage (<https://www.g3.hqusareur.army.mil>; click on *OPM Physical Scty Eqmt*).

(2) Actively participate in the operational evaluation process for FP/PS equipment to ensure a complete and accurate analysis is conducted.

(3) Notify the SEWG of any equipment they wish to have evaluated, and provide the system type, the source of information, and the desired use of the equipment.

c. The United States Army Contracting Command, Europe, and other contracting activities supporting units in the European theater will ensure that requests for procurement of nonstandard, commercial FP/PS equipment include written approval from the USAREUR PM before the procurement action is processed.

APPENDIX A REFERENCES

SECTION I REQUIRED PUBLICATIONS

AR 25-400-2, The Army Records Information Management System (ARIMS)

AR 190-5, Motor Vehicle Traffic Supervision

AR 190-11, Physical Security of Arms, Ammunition, and Explosives

AR 190-12, Military Police Working Dogs

AR 190-13, The Army Physical Security Program

AR 190-14, Carrying of Firearms and Use of Force for Law Enforcement and Security Duties

AR 190-16, Physical Security

AR 190-30, Military Police Investigations

AR 190-40, Serious Incident Report

AR 190-51, Security of Unclassified Army Property (Sensitive and Non-sensitive)

AR 190-56, The Army Civilian Police and Security Guard Program

AR 380-5 and USAREUR Supplement 1, Department of the Army Information Security Program

AR 385-64, U.S. Army Explosives Safety Program

AR 420-49 and USAREUR Supplement 2, Utility Services

AR 710-2, Inventory Management Supply Policy Below the Wholesale Level

AR 740-26, Physical Inventory Control

DA Pamphlet 25-16, Security Procedures for the Secure Telephone Unit, Third Generation (STU-III)

DA Pamphlet 25-380-2, Security Procedures for Controlled Cryptographic Items

DA Pamphlet 190-12, Military Working Dog Program

DA Pamphlet 190-51, Risk Analysis for Army Property

Technical Manual 5-811-1, Electric Power Supply and Distribution

Technical Manual 5-853-2, Security Engineering Concept Design

Technical Manual 5-853-4, Security Engineering Electronic Security Systems

AE Regulation 55-4, Safe Movement of Hazardous Goods by Surface Modes

AE Regulation 55-355, Joint Transportation and Traffic Management

AE Regulation 190-6, Registration and Control of Privately Owned Firearms and Other Weapons in Germany

AE Regulation 190-16, Installation Access Control

USAREUR Regulation 190-40, Serious Incident Report

USAREUR Regulation 190-62, Police and Investigation Services: Employment and Authority of Military Police, Unit Police, and Courtesy Patrols

USAREUR Regulation 385-64, USAREUR Explosives Safety Program

USAREUR Regulation 525-13, Antiterrorism/Force Protection: Security of Personnel, Information, and Critical Resources

USAREUR Regulation 715-3, Selecting, Training, Qualifying, Nominating, and Appointing Contracting Officer's Representatives

United States Army Corps of Engineers Guide Specification (CEGS) 02821, Fencing

CEGS 13720, Electronic Security System

CEGS 13721, Small Intrusion Detection System

CEGS 16528, Exterior Lighting Including Security and CCTV Applications

CEGS 16751, Closed Circuit Television Systems

SECTION II RELATED PUBLICATIONS

DOD Directive 5105.55, Defense Commissary Agency (DeCA)

DOD Instruction 1000.12, Procedures Governing Banking Offices on DOD Installations

DOD 5200.1-R, Information Security Program

DOD 5200.8-R and USEUCOM Supplement 1, Physical Security Program

DOD 4525.6-M, Department of Defense Postal Manual

DOD 5100.76-M, Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives

Director of Central Intelligence Agency Directive (DCID) 1/21, Manual for Physical Security Standards for Sensitive Compartmented Information Facilities (SCIF) (<http://www.fas.org/irp/offdocs/dcid1-21.htm>)

DCID 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities
(<http://www.fas.org/irp/offdocs/dcid6-9.htm>)

Defense Intelligence Agency Manual 50-3, Physical Security Standards for Sensitive Compartmented Information Facilities

Department of Defense Financial Management Regulation

AR 40-66, Medical Record Administration and Health Care Documentation

AR 60-10, Army and Air Force Exchange Service General Policies

AR 190-22, Searches, Seizures, and Disposition of Property

AR 210-7, Commercial Solicitation on Army Installations

AR 340-21, The Army Privacy Program

AR 380-19, Information Systems Security

AR 380-67, The Department of the Army Personnel Security Program

AR 420-70, Buildings and Structures

AR 525-13, Antiterrorism

AR 570-5, Manpower Staffing Standards System

AR 600-8-14, Identification Cards for Members of the Uniformed Services, Their Family Members, and Other Eligible Personnel

AR 725-50, Requisition, Receipt, and Issue System

AR 735-5, Policies and Procedures for Property Accountability

DA Pamphlet 350-38, Standards in Weapons Training

DA Pamphlet 710-2-1, Using Unit Supply System (Manual Procedures)

DA Pamphlet 710-2-2, Supply Support Activity Supply System: Manual Procedures

FM 3-19.30, Physical Security

FM 22-6, Guard Duty

Technical Bulletin 5-6350-264, Selection and Application of Joint-Services Interior Intrusion Detection System (J-SIIDS)

Military Handbook 1013/14, Selection and Application of Vehicle Barriers

AE Regulation 10-5, HQ USAREUR/7A Organization and Responsibilities

AE Regulation 380-40, Safeguarding and Controlling Communications Security Material

USAREUR Regulation 1-201, USAREUR Organizational Inspection Program

USAREUR Regulation 210-70, Personal Commercial Affairs

USAREUR Regulation 600-8-3, USAREUR Postal Operations Manual

USAREUR Regulation 600-410, Civilian Support Administration - Instatement and Transfer of Personnel

USAREUR Regulation 600-440, Civilian Support Logistics

USAREUR Regulation 600-472, Civilian Support - Police Authority, Possession, Carrying, and Use of Weapons for Personnel Assigned Guard Duties

USAREUR Regulation 600-474, Civilian Support Training and Inspection Procedures

USAREUR Regulation 600-700, Identification Cards and Individual Logistic Support

USAREUR Regulation 604-1, Foreign National Screening Program (Laredo Leader)

USAREUR Pamphlet 405-45, USAREUR Installations

USAREUR Operation Order on Force Protection

USAREUR Performance Work Statement for Contract Guard Services

USAREUR Abrams Tank System Security Guide

SECTION III PRESCRIBED FORMS

AE Form 190-13H(G), Personnel/Vehicle Record of Admission

AE Form 190-13H(I), Personnel/Vehicle Record of Admission

AE Form 190-13I, Issue of Weapons and Ammunition

AE Form 190-13L, Request for Waiver or Exception of Physical Security Requirements

AE Form 190-16A, Application for U.S. Army, Europe, Installation Pass

SECTION IV REFERENCED FORMS

SF 700, Security Container Information

DD Form 1348-6, DOD Single Line Item Requisition System Document (Manual Long-Form)

DD Form 1391, FY__, Military Construction Project Data

DA Form 410, Receipt for Accountable Form

DA Form 2028, Recommended Changes to Publications and Blank Forms

DA Form 2062, Hand Receipt/Annex Number

DA Form 2765-1, Request for Issue or Turn-In

DA Form 2806-R, Physical Security Survey Report

DA Form 2806-1-R, Physical Security Inspection Report

DA Form 3056, Report of Missing/Recovered Firearms, Ammunition, and Explosives

DA Form 3749, Equipment Receipt

DA Form 4261, Physical Security Inspector Identification Card

DA Form 4261-1, Physical Security Inspector Identification Card

DA Form 4283, Facilities Engineering Work Request - XFA, XFB, XFC

DA Form 4604-R, Security Construction Statement

DA Form 4930-R, Alarm/Intrusion Detection Record

DA Form 5513-R, Key Control Register and Inventory

DA Form 5557-R, Individual Reliability Screening and Evaluation Record

DA Form 7281-R, Command Oriented Arms, Ammunition, & Explosives Security Screening and Evaluation Record

APPENDIX B

GUIDELINES FOR DEVELOPING INSTALLATION BARRIER PLANS

B-1. GENERAL

Barrier plans are part of the overall antiterrorism plan evaluated during joint services integrated vulnerability assessments (JSIVAs) by the Defense Threat Reduction Agency (DTRA). Barrier plans consider the threat from stationary (parked) and moving vehicles. Barriers may be used to restrict parking, redirect traffic, or both. These guidelines will help installations develop and execute effective barrier plans for various threat conditions.

B-2. OBJECTIVE

The objective of a barrier plan is to provide orderly and timely security to U.S. Forces, their tenants, and all U.S. property. A clear, detailed, and rehearsed plan should reduce the manpower and time needed to execute force-protection requirements while maintaining a safe environment as the force protection condition (FPCON) level increases.

B-3. REFERENCES

- a. USEUCOM Operation Order 01-01 ((Secret Internet Protocol Router Network (SIPRNET): <http://www2.eucom.smil.mil/hq/ecsm/OPORD/OPORD0101.html>).
- b. USAREUR Regulation 525-13 (SIPRNET: <http://odcsops.hqusareur.army.smil.mil>).
- c. DTRA Antiterrorism Vulnerability Assessment Team Guidelines (SIPR: <http://www.odcsops.hqusareur.army.mil.smil/divisions/opsdiv/forceprotection/docstobeshared/Reference%20Documents/2002%20Guidelines.doc>).
- d. Local policy (if any).

B-4. BARRIER PLAN ELEMENTS

A clear and detailed barrier plan identifies the needs, resources, and associated actions, and directs various units and activities to take specific actions to secure the perimeters of installations and any other local U.S. military facilities under the operational control of the commander. Until necessary construction projects are completed, the barrier plan should provide for temporary barrier placement. The barrier plan should meet the intent and standards described in reference B-3c above and include the following:

a. Responsibilities. The local commander will develop barrier plans supported by class 4 supplies from the director of public works (DPW) and the director of logistics (DOL). The DPW and DOL are responsible for barrier emplacement. Provost marshal personnel will be responsible for quality control.

b. Design Threat Basis (DTB). The DTB of vehicle size, weight, speed, and pounds or kilograms of equivalent trinitrotoluene (TNT) will be determined based on the USEUCOM threat standard and local force protection team.

c. Plan Components. The following components must be addressed at each FPCON level in writing or illustrated in drawings:

(1) Types and Count. Identify in writing (table format) and on maps the types of barriers (for example, concrete, plastic, other material; jersey barriers, bollards, drop-down bars) and the number of each barrier type required at each emplacement location. Identify on maps the location, type, and number of all barriers currently in use.

(2) Storage Location. List the locations where barriers are stored (not in use).

(3) Purpose. Indicate the purpose of barriers at each location (for example, blocking or closing a road or gate, reducing speed (serpentine) or channeling traffic, arresting vehicles (cable beam drop arm, bollards).

(4) Movement Plan. Identify the resources needed (forklifts, trucks) to move barriers from one location to another.

(5) Privately Owned Vehicle Centralized Parking. If applicable, identify a central location for privately owned vehicle parking and a mass-transportation schedule both in writing and on the drawings.

(6) Traffic Patterns. Identify any vehicle or pedestrian rerouting due to barrier emplacement.

d. Subordinate Unit Tasks. Specify the tasks for which each unit is responsible when preparing and executing the barrier plan. For example:

- (1) The DPW will provide—
 - (a) Supplies according to barrier plans (develop a matrix).
 - (b) Representatives during the execution phase.
 - (c) An on-site maintenance team for work order and emergency work order support.
 - (d) Assistance to the DOL with emplacement equipment.
- (2) The DOL will provide—
 - (a) Support and equipment to place barriers, including operators.
 - (b) A representative during the execution phase.
 - (c) A maintenance team for generator maintenance.
- (3) The provost marshal will provide—
 - (a) Overall development of the barrier plan.
 - (b) Representatives to oversee execution and quality control.
- (4) Local tenant units will be designated to provide manpower to—
 - (a) Help with barrier emplacement.
 - (b) Fill barriers as required (for example, with water, sand).

B-5. RECOMMENDATIONS

- a. A barrier plan matrix by FPCON level (fig B-1) and by location that specifies the who, what, where, when, and how can be a significant part of a barrier plan, especially when a timeline is included.
- b. Barrier-emplacement considerations must include priorities, since it is unlikely that enough resources will be available to emplace all barriers simultaneously.
- c. While centralized barrier storage appears practical, on-site pre-positioning makes more sense. At low FPCONs, if practical, barriers may be doubled up or emplaced double high or doublewide according to the higher FPCON. It is easier to reconfigure than to draw, haul, and reconfigure.
- d. To conserve traffic-control barriers, make effective use of readily available obstacles, such as boulders and large tree trunks, backed by anchored barriers for denial barriers. Plastic water-filled barriers are a greater deterrent when also filled with sand.
- e. Denial barriers at choke points are a good counter for lesser-used routes at higher FPCONs.
- f. Barriers should be placed on the ground and not on bricks or blocks. Anchoring barriers works better on hard surfaces, while cabling together works better on ‘soft’ unprepared surfaces.
- g. Put the barrier plans in writing and show it on maps if possible.
- h. Identify alternate support units in the event that a designated support unit’s mission changes or the unit is deployed.

Force Protection Conditions Alpha and Bravo Timeline: event + hours unless otherwise noted				
Event	Timeline	Barriers	Resources	Responsible Activities
Barricade two-way traffic into separated lanes at delivery gate	E+3	8 Jersey concrete barriers	Barriers, forklifts, trucks	Provost marshal, DOL, DPW
Restrict access of main entrance to one lane	E+3	20 Jersey concrete barriers (serpentine)	Barriers, forklifts, trucks	Provost marshal, DOL, DPW
Restrict parking areas adjacent to buildings 1, 131, and 345	E+2	3 temporary drop-down bars	Signs, drop-down bars, trucks	Provost marshal, DOL

Force Protection Condition Charlie (in addition to FPCON Alpha and Bravo) Timeline: event + hours unless otherwise noted				
Event	Timeline	Barriers	Resources	Responsible Activities
Close both gates 2 and 4	E+1	Lock gate, raise bollards		Provost marshal
Restrict access of main entrance to enter only	E+3	1 drop-down bar; 4 Jersey concrete barriers; 2 tetrahedrons	Barriers, forklifts, trucks	Provost marshal, DOL, DPW
Close parking areas adjacent to buildings 1, 131, and 345	E+3	18 Jersey plastic barriers	Barriers, trucks	Provost marshal, DOL, DPW, Unit X

Force Protection Condition Delta (in addition to FPCON Charlie) Timeline: event + hours unless otherwise noted				
Event	Timeline	Barriers	Resources	Responsible Activities
Convert traffic loop to one-way traffic	E+3	10 Jersey plastic barriers	Signs, barriers, trucks	Provost marshal, DOL, DPW, Unit X
Enclave military family housing	E+6	Wire standoff @ 15 meters; 24 Jersey plastic barriers	Wire, posts, barriers, trucks	Provost marshal, DOL, DPW, Unit X

Figure B-1. Sample Matrixes

i. Public-affairs-office notification procedures for should be in place for informing the community of centralized parking and changes in traffic patterns.

j. The DTRA concept for barrier plans includes several supporting actions at higher FPCONs: enclaving, centralized parking, and a curtailment plan.

(1) Enclaving should be used for key on-post (critical or high-occupancy) facilities during higher FPCONs or for grouped buildings that require additional standoff due to physical-security requirements or structural vulnerability.

(2) Centralized parking is a denial measure that limits vehicle access on the installation by creating vehicle-exclusion areas. This may require significant guard and transportation efforts to successfully implement.

(3) A curtailment plan is the planned cessation of non-mission-essential operations. If the conduct of a unit's primary mission is temporarily changed to installation guard or other force-protection measure, a written curtailment plan is in order. If civilian operations, schools, and morale, welfare, and recreation facilities will cease operations and close, this should be included in the curtailment plan.

B-6. BARRIER GUIDELINES

The use of vehicle barriers can greatly enhance a commander's force protection posture. Careful consideration must be used in the planning and installation of the barriers. Figure B-2 is a sample drawing showing the use of different types of barriers. Table B-1 provides guidance on barrier use. Figure B-3 shows some of the different types of barriers available.



Figure B-2. Sample Drawing Showing Number and Type of Barriers

Table B-1 Barrier Guidelines (notes)						
Recommended Use	Barrier Type	Arresting Effectiveness	Easily Moved	Emplaced Quickly	Equipment Cost (\$000) Installed	DOS/DOD Impact Speed Rating
Traffic channeling and speed control	Concrete Jersey barriers	11k lb @ 30 mph	no	yes	\$0.47 to \$0.5	NA
	Plastic Jersey barriers	5k lb @ 30 mph	yes	yes	\$0.2 to \$0.3	NA
Arresting 15,000-lb truck for 9- to 14-foot lane	1. Cable crash beam - manual	15k lb @ 30 mph	no	no	\$16.00	K4
	2. Cable crash beam - hydraulic	15k lb @ 30 mph	no	no	\$26.00	K4
	3. Drum/wedge	42K lb @ 30 mph	no	no	\$43.00	K12
	4. Bollards (set of 3)	15K lb @ 30 mph	no	no	\$43.00	K8 to K12
NOTES: 1. Arresting barriers are based on stopping a vehicle weighing 15,000 pounds (lbs) and traveling 30 miles per hour (mph). These will be permanently installed. 2. Each access-control point (ACP) will be surveyed to determine the best solution for barrier combination and physical layout. Emergency vehicle and delivery truck access will be considered. 3. Concrete Jersey barriers will be positioned properly (serpentine layout) to reduce speed of vehicles to 10 mph when approaching gates. Concrete Jersey barriers can be used to block roads and gates, but must be stacked or doubled to achieve arresting standards. Concrete Jersey barriers must be anchored with 2-foot #6 steel bars (0.75-inch) for maximum effectiveness. 4. Costs are representative of industry averages and may vary depending on the specific model and site conditions. 5. For barrier design criteria and K4, K8, and K12 rating, see Technical Manual 5-853 series and Military Handbook 1013/14. 6. For active vehicle-barrier specifications, see Unified Facilities Guide Specifications (UFGS) (previously United States Army Corps of Engineers Guide Specification (CEGS) 02840) at http://www.hnd.usace.army.mil/techinfo .						


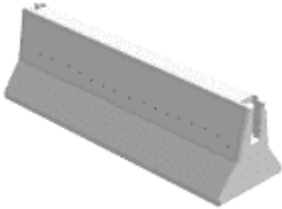
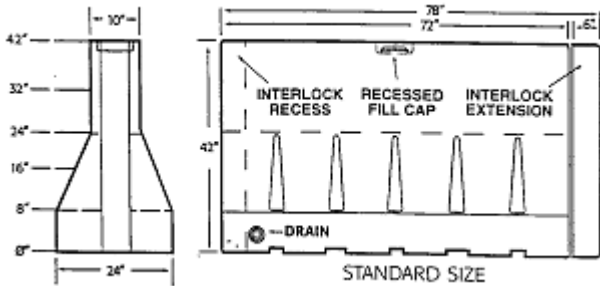


	Drop Arm/Crash Beam
	Jersey Barrier
 <p>Technical drawing of a plastic barrier. The side view shows a cross-section with a top width of 10 inches and a base width of 24 inches. The front view shows a standard size barrier with a total width of 78 inches and a height of 42 inches. Labels include: INTERLOCK RECESS, RECESSED FILL CAP, INTERLOCK EXTENSION, and DRAIN.</p>	Plastic Barrier
	Drum Wedge
	Bollards

Figure B-3. Types of Barriers

APPENDIX C
SAMPLE FORMAT FOR UNIT PHYSICAL SECURITY STANDING OPERATING PROCEDURE

This appendix provides a sample format that commanders may follow when making their physical security standing operating procedure (SOP). The SOP will apply only to those personnel under the supervision of the person signing the SOP.

DEPARTMENT OF THE ARMY
UNIT
ADDRESS
Date

(UNIT) SOP X-X

STANDING OPERATING PROCEDURES

Applicability. This SOP applies to all personnel in the *(unit)* _____.

Table of Contents (optional)

(suggested paragraph headings; modify as needed)

Purpose

References

Responsibilities

Policy

Procedures

Signature Block
Unit Commander

1. PURPOSE

This SOP establishes responsibilities and procedures for safeguarding arms, ammunition, explosives, supplies, equipment, and personnel of *unit or activity name*.

2. REFERENCES

- a. AR 190-11.
- b. AR 190-13.
- c. AR 190-51.
- d. AR 710-2.
- e. DA Pamphlet 190-51.

f. DA Pamphlet 710-2-1.

g. AE Regulation 190-13.

h. FM 3-19.30.

3. APPLICABILITY

The provisions of this SOP apply to all personnel and units assigned or attached to *unit or activity name* or residing on *installation name*.

4. RESPONSIBILITIES

a. Unit Commander. The unit commander has overall responsibility for security and accountability of all weapons, ammunition, explosives, supplies and equipment assigned/issued to the unit/activity.

b. Physical Security Officer (PSO). List the duties and responsibilities assigned to the unit PSO as listed in paragraph 1-4n of this regulation.

c. First Sergeant. List the duties and responsibilities assigned to the first sergeant by the commander based only on physical security considerations, if applicable.

d. Unit Supply Sergeant. List the duties and responsibilities assigned to the unit supply sergeant by the commander and first sergeant based only on physical security considerations, if applicable.

e. Armorer. List the duties and responsibilities assigned to the armorer by the commander, first sergeant, and supply sergeant based on physical security considerations, if applicable.

f. Civilian Personnel. Designate which, if any, civilian personnel have physical security duties and specify the duties and responsibilities for each. Use the guidance in this regulation to develop the duties for each individual, such as the primary and alternate key custodian.

5. ANNEXES

Procedures and responsibilities for each function are indicated as follows:

a. Annex A. Arms, Ammunition, and Explosives.

b. Annex B. Security of Property and Equipment.

c. Annex C. Key-and-Lock Control.

d. Annex D. Emergency Evacuation of Arms and Ammunition.

e. Annex E. Intrusion Detection System (IDS).

f. Annex F. Bomb Threat.

g. Annex G. Security of Arms, Ammunition, Explosives, Property, and Equipment in Transit.

h. Annex H. Security of Arms, Ammunition, Property, and Equipment in a Field Environment.

i. Annex I. Antiterrorism/Force Protection (AT/FP).

ANNEX A

ARMS, AMMUNITION, AND EXPLOSIVES

1. References. *List applicable references, such as regulations, field manuals, and other documents relating to the security of arms, ammunition, and explosives.*

2. Purpose. This annex establishes the responsibilities, standards, and procedures for securing arms, ammunition, and explosives in the *unit or activity name*.

3. Applicability. This annex applies to all personnel assigned or attached to the *unit or activity name*.

4. Responsibilities. *Specify the specific duties and responsibilities of the physical security officer (PSO), first sergeant, supply sergeant, armorer, and other personnel relating to the security, issue, and turn-in of arms, ammunition, and explosives, as applicable.*

5. Procedures. *Specify the manner in which weapons and ammunition will be stored in racks, containers, or cabinets in the arms room. Indicate key-and-lock control procedures for arms room keys and all inventory procedures required by regulation. Briefly describe access-control procedures and the requirements for background checks for all personnel authorized unaccompanied access to the arms room by the commander. Briefly cover ammunition management procedures or refer those personnel DA Pamphlet 710-2-1, chapter 11.*

6. Issue and Turn-In Procedures. *Specify the procedures used by the unit or activity to issue and turn-in all weapons, both individual and crew-served.*

7. Inspections and Inventories. *Specify which inspections of arms security will be conducted, the frequency and type of inventories that must be accomplished, and the procedures to follow for recording the results of the inspection and inventories.*

8. Formats and Forms. *Either attach locally formatted samples of the forms required to accomplish all tasks or refer to those in this regulation.*

ANNEX B

SECURITY OF PROPERTY AND EQUIPMENT

1. References. *List applicable references, such as AR 190-51, AR 710-2, and DA Pamphlet 710-2-1.*

2. Purpose. This annex establishes the responsibilities, standards, and procedures for safeguarding property and equipment in the *unit or activity name*.

3. Applicability. This annex applies to all personnel assigned or attached to the *unit or activity name*.

4. Responsibilities. *Designate the duties and responsibilities of the PSO, unit supply sergeant, and other personnel with respect to the security of property and equipment to ensure duties and procedures outlined are specifically identified, if applicable.*

5. Procedures. *Follow the risk-analysis procedures in DA Pamphlet 190-51 with assistance from the servicing base support battalion (BSB) physical security office or applicable agency to determine the level of risk assigned to your facility. Make use of the BSB's services for this requirement. When the level of risk is known, adhere to the protective and procedural measures in AR 190-51, chapter 3. The SOP need only refer to AR 190-51, chapter 3, for personnel to determine the protective and procedural standards associated with each category of property and equipment.*

ANNEX C

KEY-AND-LOCK CONTROL

- 1. References.** *List applicable references, such as AR 190-11, AR 190-51, and FM 3-19.30.*
 - 2. Purpose.** This annex establishes the responsibilities, standards, and procedures for identification and control of all locks, keys, and combinations used in the security of arms, ammunition, explosives, property, and equipment. *Use chapters 3 and 5 of this regulation to develop this annex.*
 - 3. Applicability.** This annex applies to all personnel assigned or attached to the *unit or activity name*.
 - 4. Responsibilities.** *Specify the responsibilities of the PSO and key/lock primary and alternate custodians, and ensure that the specific functions described in chapter 3 and 5 of this regulation are addressed.*
 - 5. Procedures.** *Describe how the unit PSO and key custodian will be appointed and how storage facilities and containers will be identified for controlled locking devices. Describe how the locking devices will be identified for inclusion in the control system and how individual soldiers will be authorized issue of keys, locks, and combinations. Include information on the temporary issue of keys, those used for personal retention by limited individuals, and the type of containers where the key custodian will secure the locks, keys, or combinations in their custody.*
 - 6. Formats.** *Refer to the appropriate formatted forms for key/lock/combination control described in chapters 3 and 5 of this regulation.*
-

ANNEX D

EMERGENCY EVACUATION OF ARMS AND AMMUNITION

- 1. References.** *List applicable references, such as AR 190-11 and FM 3-19.30.*
 - 2. Purpose.** This annex establishes the responsibilities, standards, and procedures for the emergency evacuation of arms and ammunition to a secure location in the event of a threat to the security of the arms and ammunition.
 - 3. Applicability.** This annex applies to all personnel assigned or attached to the *unit or activity name*.
 - 4. Responsibilities.** *Specify the duties of the PSO, civilian personnel, and unit personnel responsible for the emergency evacuation of weapons and ammunition.*
 - 5. Procedures.** *Identify the conditions for the emergency removal of arms and ammunition, the manner of removal, the security precautions to be used during the transportation of the arms and ammunition, the location to which the arms and ammunition will be taken, the routes to be used, and which inventory and inspection procedures to initiate to ensure that all arms and ammunition are properly accounted for during and after the evacuation.*
 - 6. Test.** *The personnel responsible for implementation must test these procedures and record the results. Testing personnel will help correct weaknesses or forward them to higher command levels for assistance in their resolution. Normally, tests are conducted without moving the arms or ammunition.*
-

ANNEX E

INTRUSION DETECTION SYSTEM (IDS)

- 1. References.** *List applicable references, such as AR 190-11, AR 190-13, and FM 3-19.30.*
- 2. Purpose.** This annex establishes the responsibilities, standards, and procedures for the operation of the IDS in the *unit or activity name* arms room.
- 3. Applicability.** This annex applies to all personnel assigned or attached to the *unit or activity name*.
- 4. Responsibilities.** *Specify the responsibilities of the PSO, supply sergeant, key custodian, and civilian personnel with respect to the control and operation of the IDS.*

5. Procedures. *Specify the procedures to be used by unit personnel for the placement of warning signs, operation of the IDS, control of IDS keys, inspections, checks, and tests of the IDS, and the documentation of such inspections, checks, and tests, both by unit personnel and the agency monitoring the system. Also identify what the unit personnel must do if the IDS alarm fails (armed-guard requirements, relocation of weapons).*

6. Forms and Formats. *See chapters 2, 3, and 5 for samples of support documentation.*

ANNEX F BOMB THREAT

1. References. *List applicable references, such as AR 190-13 and FM 3-19.30.*

2. Purpose. This annex establishes the responsibilities, standards, and procedures to be used in the event of a bomb threat against the *unit or activity name*.

3. Applicability. This annex applies to all personnel attached or assigned to the *unit or activity name*.

4. Responsibilities. *Specify the duties and responsibilities of the PSO, civilian personnel, and unit personnel regarding bomb threats.*

5. Procedures. *Specify the internal notification, external notification, and evacuation procedures to be followed in the event of a bomb threat at the unit or facility.*

6. Forms and Formats. *Use the Federal Bureau of Investigation Bomb Data Center cards. These cards may be ordered through the normal publications system.*

7. Serious Incident Reports (SIRs). *Meet the SIR requirements in AR 190-40, USAREUR Regulation 190-40, and local command procedures.*

ANNEX G SECURITY OF ARMS, AMMUNITION, EXPLOSIVES, PROPERTY, AND EQUIPMENT IN TRANSIT

1. References. *List applicable references, such as AR 190-11, DA Pamphlet 710-2-1, FM 3-19.30, and AE Regulation 55-4.*

2. Purpose. This annex establishes the responsibilities, standards, and procedures to be used to secure arms, ammunition, explosives, property, and equipment during transportation.

3. Applicability. This annex applies to all personnel assigned or attached to the *unit or activity name*.

4. Responsibilities. *Specify the duties and responsibilities of the PSO, unit supply sergeant, armorer, civilian personnel, and convoy commander with respect to the security of arms, ammunition, explosives, property, and equipment while in transit.*

5. Procedures. *Specify the vehicles in which arms, ammunition, explosives, property, and equipment may be transported, the specific type of equipment, arms, or ammunition requiring security during transit, the requirement for armed guards (if applicable), the types and number of locks required to secure the equipment, the number of personnel and their grade needed to accomplish the mission, and inventory and accountability procedures to be used from the start until completion of the mission.*

ANNEX H

SECURITY OF ARMS, AMMUNITION, PROPERTY, AND EQUIPMENT IN A FIELD ENVIRONMENT

1. References. *List applicable regulations, such as AR 190-11, DA Pamphlet 710-2-1, and FM 3-19.30.*

2. Purpose. This annex establishes the responsibilities, standards, and procedures for securing arms, ammunition, property, and equipment in a field environment.

3. Applicability. This annex applies to all personnel assigned or attached to the *unit or activity name*.

4. Responsibilities. *Specify the duties and responsibilities of the unit PSO, first sergeant, armorer, key custodian, civilian personnel, and individual soldiers for securing arms, ammunition, property, and equipment in a field environment.*

5. Procedures. *Specify the procedures to be used for securing arms, ammunition, property, and equipment while in a controlled, consolidated location when issued to the individual soldier. Make specific reference to the manner by which the individual soldier is expected to secure his or her weapon and ammunition. Develop separate inventory and key-and-lock procedures for the field environment.*

ANNEX I

ANTITERRORISM/FORCE PROTECTION (AT/FP)

1. References. *List applicable references, such as AR 190-51, AR 525-13, and USAREUR Regulation 525-13.*

2. Purpose. This annex establishes the responsibilities, standards, and procedures for force protection in the *unit or activity name*.

3. Applicability. This annex applies to all personnel assigned or attached to the *unit or activity name*.

4. Responsibilities. *Specify the duties and responsibilities of the PSO, other officers, and noncommissioned officers assigned security responsibilities for force protection.*

5. Procedures. *Specify the procedures to be used in planning and implementing force protection measures with the unit or facility. Address the different force protection conditions (FPCONs) and what procedures will be followed for each measure. Use USAREUR Regulation 525-13 to develop the duties and procedures.*

APPENDIX D

INSTRUCTIONS FOR COMPLETING AE FORM 190-13L

This appendix provides instructions for completing AE Form 190-13L.

Part I. Requesting units or activities will complete part 1 as follows:

Address Blocks. In the “FROM” box, enter the mailing address of the requesting organization; in the “TO” box, enter the mailing address of the supporting base support battalion (BSB) provost marshal office.

Block 1, REQUEST. Place an X on the appropriate line indicating whether the request is in reference to a *waiver* or *exception*.

Block 2, TYPE OF REQUEST. Indicate whether the request is an *initial*, a request for *extension*, a request for a *change* to an approved request, or a *cancellation* of an approved request.

Block 3, BRIEF DESCRIPTION OF SPECIFIC REQUIREMENT FOR WHICH EXCEPTION OR WAIVER IS REQUESTED. Cite the specific regulatory requirement by paragraph and line number that the waiver or exception applies to.

Block 4, BRIEF DESCRIPTION OF ACTUAL DEFICIENCY. Describe the deficiency (for example, the walls are made of cardboard and do not meet the minimum structure standards for a secure storage area) and attach additional documentation that may further support the request. Identify the location of facility (for example, arms room located in an occupied troop billets or unoccupied building, or located on a U.S.-occupied or unoccupied installation).

Block 5, PROPOSED CORRECTIVE ACTION. Explain the action being taken to correct deficiencies (for example, a building meeting the construction standards is being built and is scheduled to be completed in 6 months).

Block 6, DESCRIBE COMPENSATORY MEASURES IN PLACE UNTIL DEFICIENCY IS CORRECTED OR EXCEPTION IS GRANTED. List the compensatory measures being taken until the deficiencies can be corrected. Ensure the security being provided meets or exceeds the requirements of the applicable regulation (for example, the equipment is being stored in a metal container express (CONEX) that is secured using GSA-approved secondary padlocks, the CONEX is surrounded by a standard security fence with security lighting, and the area is checked by security guards once every hour).

Block 7, WORKORDER NO./PRIORITY. State the project number (work order number) provided by the area support group (ASG) or BSB directorate of public works (DPW) and the priority assigned to the project.

Block 8, ESTIMATED COMPLETION DATE. Indicate expected date deficiencies will be corrected.

Block 9, TOTAL ESTIMATED COST. Provide an estimated cost of the corrective action, if applicable.

Block 10, POINT OF CONTACT. Identify a unit or organization POC that knows the details of the request.

Block 11, RANK/NAME OF COMMANDER/OIC. Enter the rank and name of the requesting unit’s commander or officer in charge (OIC).

Block 12, SIGNATURE. Have the commander or OIC sign the request.

Block 13, DATE. Enter the date of the request.

Part II. The BSB provost marshal will review the request, recommend approval or disapproval, and may attach comments. After completing part II, the BSB Provost marshal will forward the request to the ASG provost marshal.

Part III. The ASG Provost marshal will review the request, recommend approval or disapproval, and may attach comments. After completing part III the ASG provost marshal will forward the request to the Security Operations Branch, Office of the Provost Marshal (OPM), HQ USAREUR/7A.

Part IV. The OPM will complete parts VI (and V if the request is for a USAREUR requirement). If the request is for a waiver or exception to an Army requirement, the OPM will review the request, recommend approval or disapproval, and send the action to HQDA for a final decision.

NOTE: The OPM will assign a control number to track the request (block 34). Any future correspondence about the waiver or exception request must include the this control number.

Part V. HQDA (DAMO-ODL-S) will complete part V when the request is for a waiver or exception to an Army requirement.

APPENDIX E

INSTRUCTIONS FOR COMPLETING AE FORM 190-13I

This appendix provides instructions for completing AE Form 190-13I.

Block 1, UNIT OR STATION. Self-explanatory.

Block 2, RACK NUMBER. The unit armorer or issuing authority should print the rack (also known as the weapon number assigned by the unit) from which the weapon is taken. If the weapon is not from a rack, the number of the secure storage container should be printed in this block.

Block 3, TYPE OF WEAPON. The unit armorer will list the nomenclature of the weapon (for example, M16A1). Bayonets issued with weapons should also be listed (for example, M16A1w/B).

Block 4, SERIAL NUMBER. Enter the weapon serial number.

Block 5, NUMBER ROUNDS. Self-explanatory. If no rounds were issued, then 0 will be entered in this block. Block 5 should not be blank.

Block 6, DATE OUT and TIME OUT. The person accepting the weapon will enter the date and time that the weapon is issued.

Block 7, PRINTED NAME AND SIGNATURE. The person accepting the weapon will print and sign his or her name.

Block 8, OUT BY (INITIAL). The issuing armorer will enter his or her initials after ensuring that all weapon information is correct.

Block 9, DATE IN and TIME IN. The person turning in the weapon will enter the date and time the weapon is turned in.

Block 10, NUMBER ROUNDS. The armorer will enter the number of rounds being turned in. If no rounds were turned in, 0 will be entered. Block 10 should never be blank.

Block 11, TURNED IN TO (SIGNATURE). The armorer receiving the weapon will sign for the weapon.

Block 12, TURNED IN BY (INITIAL). The person turning in the weapon will enter his or her initials.

GLOSSARY

AA&E	arms, ammunition, and explosives
AAR	after-action report
ACP	access-control point
ADP	automated data processing
AHA	ammunition holding area
AMG	Alarm Monitoring Group
AOR	area of responsibility
ASG	area support group
ASI	additional skill identifier
ASL	authorized stockage list
ASP	ammunition supply point
AST	area support team
AT/FP	antiterrorism/force protection
BASOPS	base operations
BMM	borrowed military manpower
BOLO	be on the lookout
BSB	base support battalion
CAC	common access card
CCI	controlled cryptographic item
CCTV	closed-circuit television
CEGS	United States Army Corps of Engineers Guide Specification
CG, USAREUR/7A	Commanding General, United States Army, Europe, and Seventh Army
CIDS	commercial intrusion detection system
CIM	centralized installation management
CN	chloroacetophenone
COE	Chief of Engineers
COMSEC	communications security
CONEX	container express
CONUS	continental United States
COR	contracting officer's representative
CPAC	civilian personnel advisory center
CPS	capacitance proximity sensor
CRC	crime records check
CS	ortho-chlorobenzal malononitrile
DA	Department of the Army
DCG/CofS, USAREUR/7A	Deputy Commanding General/Chief of Staff, United States Army, Europe, and Seventh Army
DCID	Director of Central Intelligence directive
DCII	Defense Central Intelligence Index
DEROS	date eligible to return from overseas
DOD	Department of Defense
DOIM	director of information management
DOL	director of logistics
DOS	Department of State
DPW	director of public works
DS	duress sensor
DSN	Defense Switched Network
DTB	design threat basis
DTRA	Defense Threat Reduction Agency
EDD	explosive detector dog
EECS	electronic entry/access control system
ESS	electronic security system
ETS	expiration term of service
FM	field manual
FP	force protection
FPCON	force protection condition
G1	Office of the G1, HQ USAREUR/7A
G2	Office of the G2, HQ USAREUR/7A

G3	Office of the G3, HQ USAREUR/7A
G6	Office of the G6, HQ USAREUR/7A
G8	Office of the G8, HQ USAREUR/7A
GSA	General Services Administration
HDT	high-density target
HQDA	Headquarters, Department of the Army
HQ USAREUR/7A	Headquarters, United States Army, Europe, and Seventh Army
HRP	high-risk personnel
HVT	high-value target
IACS	Installation Access Control System
I-CIDS	Integrated Commercial Intrusion Detection System
IDS	intrusion detection system
IMA-Europe	United States Army Installation Management Agency, Europe Region Office
IRP	Individual Reliability Program
JAWG	Joint Antiterrorism Working Group
J-SIIDS	Joint-Services Interior Intrusion Detection System
JSIVA	joint services integrated vulnerability assessment
LAR	logistics assistance representative
LAW	light anti-tank weapon
lb	pound
MACOM	major Army command
MAL	master authorization list
MCA	Military Construction, Army
MEVA	mission-essential vulnerable area
MI	military intelligence
MILSTRIP	Military Standard Requisitioning and Issue Procedures
mm	millimeter
MP	military police
mph	miles per hour
MTOE	modification table of organization and equipment
MWD	military working dog
NAC	national agency check
NACI	national agency check and written inquiries
NATO	North Atlantic Treaty Organization
NCEL	Naval Civil Engineering Laboratory
NCIC	National Crime Information Center
NCO	noncommissioned officer
NSN	national stock number
OCIE	organizational clothing and individual equipment
OMA	Operations and Maintenance, Army
OPA	Other Procurement, Army
OPM	Office of the Provost Marshal, HQ USAREUR/7A
PCS	permanent change of station
PIN	personal identification number
PIR	passive infrared
PM	Provost Marshal, USAREUR
PM-PSE	Office of the Program Manager - Physical Security Equipment
POC	point of contact
POL	petroleum, oils, and lubricants
PS	physical security
PSE	physical security equipment
PSI	physical security inspector
PSO	physical security officer
PUS	passive ultrasonic sensor
PWS	performance work statement
QAE	quality assurance evaluator
QASAS	quality assurance specialist (ammunition surveillance)
RAM	random antiterrorism measure
ROE	rules of engagement

SAV	staff-assistance visit
SAW	squad automatic weapon
SCIF	sensitive compartmented information facility
SCOR	site contracting officer's representative
SD	shock detector
SEWG	USAREUR Security Equipment Working Group
SF	standard form
SIPRNET	Secret Internet Protocol Router Network
SIR	serious incident report
SMAW-D	shoulder-launched multipurpose assault weapon
SMS	Security Management System
SOFA	Status of Forces Agreement
SOP	standing operating procedure
STC	senior tactical commander
TASC	training and audiovisual support center
TDA	table of distribution and allowances
TDY	temporary duty
TISA	troop issue subsistence activity
TNT	trinitrotoluene
TOW	tube-launched, optically tracked, wire-guided
UCMJ	Uniform Code of Military Justice
UFGS	Unified Facilities Guide Specifications
UMS	ultrasonic motion sensor
U.S.	United States
USACE	United States Army Corps of Engineers
USACIDC	United States Army Criminal Investigation Command
USAMPS	United States Army Military Police School
USAREUR	United States Army, Europe
USEUCOM	United States European Command